(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 806 526 A1

(12) **EUROPEAN PATENT APPLICATION**
published in accordance with Art. 153(4) EPC

(43) Date of publication:
**26.11.2014 Bulletin 2014/48**

(21) Application number: **12865737.6**

(22) Date of filing: **05.11.2012**

(51) Int Cl.:
***H02J 7/02*** *(2006.01)* ***B60L 11/18*** *(2006.01)*
***H01M 10/48*** *(2006.01)* ***H02J 7/00*** *(2006.01)*

(86) International application number:
**PCT/JP2012/007076**

(87) International publication number:
**WO 2013/108318 (25.07.2013 Gazette 2013/30)**

(84) Designated Contracting States:
**AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR**

(30) Priority: **17.01.2012 JP 2012007476**

(71) Applicant: **Panasonic Corporation**
**Kadoma-shi, Osaka 571-8501 (JP)**

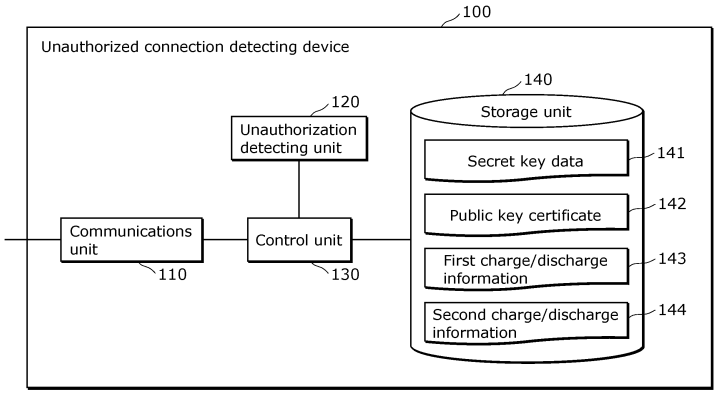
(72) Inventors:
- **UNAGAMI, Yuji**
  **Osaka 540-6207 (JP)**
- **MATSUZAKI, Natsume**
  **Osaka 540-6207 (JP)**
- **OHMORI, Motoji**
  **Osaka 540-6207 (JP)**

(74) Representative: **Vigand, Philippe et al**
**Novagraaf International SA**
**3 chemin de l'Echo**
**1213 Onex Geneva (CH)**

# (54) UNAUTHORIZED CONNECTION DETECTION DEVICE, UNAUTHORIZED CONNECTION DETECTION SYSTEM AND METHOD FOR DETECTING UNAUTHORIZED CONNECTION

(57) An unauthorized connection detecting device (100), which detects whether or not a power storage device is an unauthorized power storage device, includes: a communications unit (110) receiving first charge/discharge information in which first identification information and first connection information are associated each other, the first identification information identifying an encryption key of the power storage device used for mutual authentication between a charge/discharge device (200) and the power storage device, and the first connection information being on the power storage device and obtained when the power storage device is connected to the charge/discharge device (200); and an unauthorization detecting unit (120) detecting whether or not the power storage device is the unauthorized power storage device, by determining, using the first identification information and the first connection information, whether or not two or more power storage devices associated with a single first identification information item are present.

FIG. 2




EP 2 806 526 A1

## Description

[Technical Field]

**[0001]** The present invention relates to an unauthorized connection detecting device, an unauthorized connection detecting system, and an unauthorized connection detecting method for detecting whether or not a power storage device connectable to a charge/discharge device for charging or discharging with power is an unauthorized power storage device or whether or not the charge/discharge device is an unauthorized charge/discharge device.

[Background Art]

**[0002]** In recent years, secondary batteries are used for various purposes such as electric vehicles. The secondary batteries are included in a device (hereinafter referred to as power storage device), such as an electric vehicle. The power storage device is connected to a charge/discharge device to be charged or discharged. In relation to the above technique, some conventional techniques have been proposed to prevent a connection to an unauthorized power storage device or an unauthorized charge/discharge device (see Patent Literatures 1 and 2, for example).

[Citation List]

[Patent Literature]

**[0003]**

[PTL 1]
Japanese Patent No. 4407753
[PTL 2]
Japanese Unexamined Patent Application Publication No. 2010-200528

[Summary of Invention]

[Technical Problem]

**[0004]** The above conventional techniques have a problem in that the techniques cannot detect such an unauthorized power storage device or an unauthorized charge/discharge device, and thus fail to prevent the connection to the unauthorized power storage device or the unauthorized charge/discharge device.

**[0005]** The present invention provides an unauthorized connection detecting device, an unauthorized connection detecting system, and an unauthorized connection detecting method which are capable of detecting an unauthorized power storage device or an unauthorized charge/discharge device that have a cryptographic module of an authentic product introduced thereinto in an unauthorized manner.

[Solution to Problem]

**[0006]** An unauthorized connection detecting device according to an aspect of the present invention detects whether or not a power storage device that is connectable to a charge/discharge device for charging or discharging with power is an unauthorized power storage device. The unauthorized connection detecting device includes: a communications unit which receives first charge/discharge information in which first identification information and first connection information are associated each other, the first identification information being information for identifying an encryption key of the power storage device used for mutual authentication between the charge/discharge device and the power storage device connectable to the charge/discharge device, and the first connection information being information on the power storage device and obtained when the power storage device is connected to the charge/discharge device; and an unauthorization detecting unit which detects whether or not the power storage device connected to the charge/discharge device is the unauthorized power storage device, by determining, using the first identification information and the first connection information included in the received first charge/discharge information, whether or not two or more power storage devices associated with a single first identification information item are present.

**[0007]** It is noted that such a general and specific aspect may be implemented in the form of a system, a method, an integrated circuit, a computer program, or a non-transitory computer-readable recording medium such as a CD-ROM, or any combination of systems, methods, integrated circuits, computer programs, or computer-readable recording media.

[Advantageous Effects of Invention]

**[0008]** The present invention successfully implements an unauthorized connection detecting device which is capable of detecting an unauthorized power storage device or an unauthorized charge/discharge device that have a cryptographic module of an authentic product introduced thereinto in an unauthorized manner.

[Brief Description of Drawings]

**[0009]**

[Fig. 1]
FIG. 1 shows a structure of an unauthorized connection detecting system including an unauthorized connection detecting device according to an embodiment.

[Fig. 2]
FIG. 2 depicts a block diagram showing a functional structure of the unauthorized connection detecting device according to the embodiment.

[Fig. 3]
FIG. 3 exemplifies first charge/discharge information according to the embodiment.
[Fig. 4]
FIG. 4 exemplifies second charge/discharge information according to the embodiment.
[Fig. 5]
FIG. 5 depicts a block diagram showing a functional structure of a charge/discharge device according to the embodiment.
[Fig. 6]
FIG. 6 depicts a block diagram showing a functional structure of a power storage device according to the embodiment.
[Fig. 7]
FIG. 7 depicts a flowchart exemplifying an operation performed by the charge/discharge device according to the embodiment.
[Fig. 8]
FIG. 8 depicts a flowchart exemplifying an operation performed by the power storage device according to the embodiment.
[Fig. 9]
FIG. 9 depicts a flowchart exemplifying mutual authentication processing performed by the charge/discharge device and the power storage device according to the embodiment.
[Fig. 10]
FIG. 10 depicts a flowchart exemplifying an operation of how the unauthorized connection detecting device according to the embodiment detects an unauthorized power storage device.
[Fig. 11]
FIG. 11 depicts a flowchart exemplifying an operation of how the unauthorized connection detecting device according to the embodiment detects an unauthorized charge/discharge device.
[Fig. 12]
FIG. 12 depicts a flowchart exemplifying an operation of how the unauthorized connection detecting device according to Modification 1 of the embodiment detects an unauthorized charge/discharge device.
[Fig. 13]
FIG. 13 depicts a flowchart exemplifying mutual authentication processing performed by the charge/discharge device and the power storage device according to Modification 2 of the embodiment.
[Fig. 14]
FIG. 14 depicts a block diagram showing a minimal structure of the unauthorized connection detecting device according to the embodiment and Modifications thereof.

[Description of Embodiment]

[Underlying Knowledge Forming Basis of the Present Invention]

**[0010]** In the case where a power storage device or a charge/discharge device is not an authentic one but unauthorized one, such unauthorized devices could have performance problems, burst into flame, and cause electric leakage, and could be misused for theft of electricity. Moreover, when the unauthorized power storage device and the unauthorized charge/discharge device are connected with each other, information may be exchanged therebetween. The exchange could cause the leakage of the information.

**[0011]** In relation to the above problems, some conventional techniques have been proposed to prevent a connection to an unauthorized power storage device or an unauthorized charge/discharge device (see Patent Literatures 1 and 2, for example). In order to prevent an unauthorized connection, the techniques involve mutual authentication between a power storage device and a charge/discharge device to determine whether the charge/discharge device can or cannot charge the power storage device.

**[0012]** However, the inventor has found out that the above conventional techniques have the after-described problem. Specifically, the problem is that the above conventional techniques are unable to detect an unauthorized power storage device or an unauthorized charge/discharge device, and thus might not be able to prevent a connection to the unauthorized power storage device or the unauthorized charge/discharge device.

**[0013]** In other words, when a cloned cryptographic module (a secret key and a public key certificate) of an authentic product is introduced into an unauthentic power storage device or an unauthentic charge/discharge device in an unauthorized manner, the clone allows the unauthentic power storage device or charge/discharge device to receive mutual authentication. As a result, the unauthentic power storage device or charge/discharge device cannot be detected. Hence, the conventional techniques cannot prevent a connection to the unauthentic and unauthentic power storage device or charge/discharge device.

**[0014]** In order to solve the above problems, an unauthorized connection detecting device according to an implementation of the present invention detects whether or not a power storage device that is connectable to a charge/discharge device for charging or discharging with power is an unauthorized power storage device. The unauthorized connection detecting device includes: a communications unit which receives first charge/discharge information in which first identification information and first connection information are associated each other, the first identification information being information for identifying an encryption key of the power storage device used for mutual authentication between the charge/dis-

charge device and the power storage device connectable to the charge/discharge device, and the first connection information being information on the power storage device and obtained when the power storage device is connected to the charge/discharge device; and an unauthorization detecting unit which detects whether or not the power storage device connected to the charge/discharge device is the unauthorized power storage device, by determining, using the first identification information and the first connection information included in the received first charge/discharge information, whether or not two or more power storage devices associated with a single first identification information item are present.

**[0015]** Hence, the unauthorized connection detecting device detects whether or not a power storage device is an unauthorized power storage device by (i) receiving the first charge/discharge information in which the first identification information for identifying a secret key of a power storage device and the first connection information on a power storage device are associated each other, and (ii) determining, based on the first charge/discharge information, whether or not two or more power storage devices associated with a single first identification information are present. Here, on authentic power storage devices, a single first identification information item is assigned to one power storage device. When a cryptographic module of an authentic product is introduced in an unauthorized manner, however, two or more power storage devices associated with a single first identification information item are to be present. Hence, in the case where two or more power storage devices associated with a single first identification information are present, the unauthorized connection detecting device 100 can determine that any one or more of the power storage devices are unauthorized ones. Thus, the unauthorized connection detecting device can detect an unauthorized power storage device having a cryptographic module of an authentic product introduced in an unauthorized manner.

**[0016]** For example, the communications unit may receive the first charge/discharge information in which the first identification information and the first connection information are associated each other, the first connection information including information indicating a time and a position when and where the power storage device was charged or discharged, and the unauthorization detecting unit may detect whether or not the power storage device connected to the charge/discharge device is the unauthorized power storage device, by determining, based on a relationship between times and positions included in a first connection information item associated with a single first identification information item, whether or not two or more power storage devices associated with the single first identification information item are present, the first connection information item being included in the first connection information, and the first connection information item and the single first identification information item being included in the received first charge/discharge information.

**[0017]** Thus, the unauthorized connection detecting device detects whether or not a power storage device is an unauthorized power storage device by determining, based on a relationship between times and positions associated with a single first identification information item, whether or not two or more power storage devices associated with the single first identification information item are present. In other words, in the case where there is an unnatural relationship between times and positions associated with a single first identification information item, the unauthorized connection detecting device determines that two or more power storage devices associated with the single first identification information item are present. For example, in the case where a power storage device cannot possibly travel a distance between two positions within a time period between two times when the two positions and the two times are associated with a single first identification information item, the unauthorized connection detecting device determines that two or more power storage devices associated with the single first identification information item are present. Thus, the unauthorized connection detecting device can detect an unauthorized power storage device having a cryptographic module of an authentic product introduced in an unauthorized manner.

**[0018]** For example, the communications unit may receive the first charge/discharge information in which the first identification information, time information, and position information are associated one another, the time information indicating a time when the charge/discharge device charged or discharged the power storage device, and the position information indicating a position where the charge/discharge device was.

**[0019]** Information on a time included in the first charge/discharge information received by the unauthorized connection detecting device is time information indicating the time at which a charge/discharge device charges or discharges a power storage device. Information on a position is position information such as global positioning system (GPS) information indicating a position of the charge/discharge device. Since the above features allow the unauthorized connection detecting device to receive easily created first charge/discharge information, the unauthorized connection detecting device can easily detect an unauthorized power storage device having a cryptographic module of an authentic product introduced in an unauthorized manner.

**[0020]** An unauthorized connection detecting device according to an implementation of the present invention detects whether or not a charge/discharge device that is connectable with a power storage device and charges or discharges the power storage device is an unauthorized charge/discharge device. The unauthorized connection detecting device may include: a communications unit which receives second charge/discharge information in which second identification information and second connection information are associated each other, the sec-

ond identification information being information for identifying an encryption key of the charge/discharge device used for mutual authentication between the power storage device and the charge/discharge device connectable with the power storage device, and the second connection information being information on the charge/discharge device and obtained when the charge/discharge device is connected with the power storage device; and an unauthorization detecting unit which detects whether or not the charge/discharge device connected with the power storage device is the unauthorized charge/discharge device, by determining, using the second identification information and the second connection information included in the received second charge/discharge information, whether or not two or more charge/discharge devices associated with a single second identification information item are present.

**[0021]** Thus, the unauthorized connection detecting device detects whether or not a charge/discharge device is an unauthorized charge/discharge device, by (i) receiving the second charge/discharge information in which the second identification information and the second connection information are associated each other, and (ii) determining, using the second charge/discharge information, whether or not two or more charge/discharge devices associated with a single second identification information are present. The second identification information is for identifying the encryption key of the charge/discharge device, and the second connection information is on the charge/discharge device. Here, on authentic charge/discharge devices, a single second identification information item is assigned to one charge/discharge device. When a cryptographic module of an authentic product is introduced in an unauthorized manner, however, two or more charge/discharge devices associated with a single second identification information item are to be present. Hence, in the case where two or more charge/discharge devices associated with a single second identification information are present, the unauthorized connection detecting device 100 can determine that any one or more of the power storage devices are unauthorized ones. Thus, the unauthorized connection detecting device can detect an unauthorized charge/discharge device having a cryptographic module of an authentic product introduced in an unauthorized manner.

**[0022]** For example, the communications unit may receive the second charge/discharge information in which the second identification information and the second connection information are associated each other, the second connection information including charge/discharge device identification information identifying the charge/discharge device, and the unauthorization detecting unit may detect whether or not the charge/discharge device connected with the power storage device is the unauthorized charge/discharge device, by determining whether or not two or more charge/discharge device identification information items, included in a second connection information item associated with a single second identification information item, indicate mutually different charge/discharge devices, thereby determining whether or not two or more charge/discharge devices associated with the single second identification information item are present, the two or more charge/discharge device identification information items being included in the charge/discharge device identification information, the second connection information item being included in the second connection information, and the second connection information item and the single second identification item being included in the received second charge/discharge information.

**[0023]** Thus, the unauthorized connection detecting device detects whether or not a charge/discharge device is an unauthorized charge/discharge device, by determining whether or not two or more charge/discharge device identification information items associated with a single second identification information item indicate mutually different charge/discharge devices, thereby determining whether or not two or more charge/discharge devices associated with the single second identification information item are present. In other words, in the case where two or more charge/discharge device identification information items associated with a single second identification information item indicate different charge/discharge devices, the unauthorized connection detecting device determines that two or more charge/discharge devices associated with the single second identification information item are present. Thus, the unauthorized connection detecting device can detect an unauthorized charge/discharge device having a cryptographic module of an authentic product introduced in an unauthorized manner.

**[0024]** For example, the communications unit may receive the second charge/discharge information in which the second identification information and the second connection information are associated each other, the second connection information including, as the charge/discharge device identification information, position information indicating a position of the charge/discharge device, and the unauthorization detecting unit may detect whether or not the charge/discharge device connected with the power storage device is the unauthorized charge/discharge device, by determining whether or not two or more position information items, included in a second connection information item associated with a single second identification information item, indicate mutually different positions, thereby determining whether or not two or more charge/discharge devices associated with the single second identification information item are present, the two or more position information items being included in the position information, the second connection information item being included in the second connection information, and the second connection information item and the single second identification information item being included in the received second charge/discharge information.

**[0025]** Thus, the charge/discharge device identifica-

tion information included in the second charge/discharge information received by the unauthorized connection detecting device is position information indicating the position of a charge/discharge device. The unauthorized connection detecting device detects whether or not a charge/discharge device is an unauthorized charge/discharge device, by determining whether or not two or more position information items associated with a single second identification information item indicate mutually different positions, thereby determining whether or not two or more charge/discharge devices associated with the single second identification information item are present. The two or more position information items are included in the position information. Here, the charge/discharge device is provided at a predetermined position, and never found at two or more places. Hence, in the case where two or more position information items associated with a single second identification information item indicate different positions each other, the unauthorized connection detecting device determines that two or more charge/discharge devices associated with the single second identification information item are present. Thus, the unauthorized connection detecting device can detect an unauthorized charge/discharge device having a cryptographic module of an authentic product introduced in an unauthorized manner.

**[0026]** For example, the communications unit may receive the second charge/discharge information in which the second identification information and the second connection information are associated each other, the second connection information including direct current information indicating, as the charge/discharge device identification information, a fluctuation of a direct current provided from the charge/discharge device, and the unauthorization detecting unit may detect whether or not the charge/discharge device connected with the power storage device is the unauthorized charge/discharge device, by determining whether or not two or more direct current information items, included in a second connection information item associated with a single second identification information item, indicate mutually different fluctuations, thereby determining whether or not two or more charge/discharge devices associated with the single second identification information item, the two or more direct current information items being included in the direct current information, the second connection information item being included in the second connection information, and the second connection information item and the single second identification information item being included in the received second charge/discharge information.

**[0027]** Thus, the charge/discharge device identification information included in the second charge/discharge information received by the unauthorized connection detecting device may be direct current information indicating a fluctuation of a direct current provided from a charge/discharge device. The unauthorized connection detecting device may detect whether or not a charge/discharge device is an unauthorized charge/discharge device, by determining whether or not two or more direct current information items associated with a single second identification information item indicate mutually different fluctuations, thereby determining whether or not two or more charge/discharge devices associated with the single second identification information item are present. The two or more direct current information items are included in the direct current information. Here, a direct current provided from a charge/discharge device has fluctuation which is unique to the charge/discharge device itself. Through the analysis of the fluctuation using a phase sample of the direct current, the charge/discharge device can be identified. Hence, in the case where two or more direct current information items associated with a single second identification information item indicate different fluctuations each other, the unauthorized connection detecting device determines that two or more charge/discharge devices associated with the single second identification information item are present. Thus, the unauthorized connection detecting device can detect an unauthorized charge/discharge device having a cryptographic module of an authentic product introduced in an unauthorized manner.

**[0028]** For example, the communications unit may receive the second charge/discharge information in which the second identification information and the second connection information are associated each other, the second connection information including the power storage device identification information identifying the power storage device connected to the charge/discharge device, and the unauthorization detecting unit may detect whether or not the charge/discharge device connected with the power storage device is the unauthorized charge/discharge device, by determining whether or not the number of power storage devices, identified by two or more power storage device identification information items included in a second connection information item associated with a single second identification information item, is larger than or equal to a predetermined threshold, thereby determining whether or not two or more charge/discharge devices associated with the single second identification information item are present, the two or more power storage device identification information items being included in the power storage device identification information, the second connection information item being included in the second connection information, and the second connection information item and the single second identification information item being included in the received second charge/discharge information.

**[0029]** Thus, the unauthorized connection detecting device detects whether or not a charge/discharge device is an unauthorized charge/discharge device, by determining whether or not the number of power storage devices, identified by two or more power storage device identification information items associated with a single second identification information item, is larger than or equal to a predetermined threshold, thereby determining

whether or not two or more charge/discharge devices associated with the single second identification information item are present. Here, the two or more power storage device identification information items being included in the power storage device identification information. Here, the number of power storage devices to be connected to one charge/discharge device is limited. In the case where the number of the connected power storage devices is larger than or equal to a predetermined threshold, two or more charge/discharge devices associated with a single second identification information item are to be present. In other words, in the case where the number of power storage devices associated with a single second identification information item is larger than or equal to a predetermined threshold, the unauthorized connection detecting device 100 determines that two or more charge/discharge devices associated with the single second identification information item are present. Thus, the unauthorized connection detecting device can detect an unauthorized charge/discharge device having a cryptographic module of an authentic product introduced in an unauthorized manner.

**[0030]** For example, he communications unit may receive information via one of a communications network connected with a charge station for charging the power storage device when the power storage device is connected and a communications network connected to the charge/discharge device.

**[0031]** Thus, the unauthorized connection detecting device receives information via the communications network connected either with the charging station or a charge/discharge device. In other words, when a power storage device is either charged at the charging station or one of charged and discharged by a charge/discharge device, the unauthorized connection detecting device can easily receive the information. Thus, the unauthorized connection detecting device can easily obtain information and detect an unauthorized charge/discharge device having a cryptographic module of an authentic product introduced in an unauthorized manner.

**[0032]** It is noted that the present invention can be implemented not only as the unauthorized connection detecting device but also as (i) an unauthorized connection detecting system including a charge/discharge device and an unauthorized connection detecting device which detects whether or not a power storage device connectable to the charge/discharge deice is an unauthorized power storage device or (ii) a power storage device and an unauthorized connection detecting device which detects whether or not a charge/discharge device for charging or discharging the power storage device is an unauthorized charge/discharge device.

**[0033]** In addition, the present invention can be implemented in the form of an unauthorized connection detecting method including characteristic processing carried out by the unauthorized connection detecting device or the unauthorized connection detecting system as steps. Moreover, the steps included in the unauthorized connection detecting method may be implemented in the form of a program to be executed by a computer and a computer-readable recording medium in which the program is stored. As a matter of course, the program may be distributed via a recording medium such as a CD-ROM and a transmission medium such as the Internet. In addition, the present invention may be implemented in the form of an integrated circuit having characteristic processing units included in the unauthorized connection detecting device. The present invention may be implemented in the form of any given combinations of the device, the method, the integrated circuit, the computer program, and the recording medium.

**[0034]** Described hereinafter is an embodiment with reference to the drawings. It is noted that the embodiment below shows general or specific examples. The numerical values, shapes, materials, constituent elements, arrangement positions and connecting schemes of the constituent elements, steps, and an order of steps all described in the embodiment are mere examples, and shall not limit the scope of the present invention. Among the constituent elements in the embodiment, constituent elements not recited in any one of the in dependent claims are described as arbitrary constituent elements.

**[0035]** FIG. 1 shows a structure of an unauthorized connection detecting system 10 including an unauthorized connection detecting device 100 according to the embodiment.

**[0036]** As shown in FIG. 1, the unauthorized connection detecting system 10 includes the unauthorized connection detecting device 100, a charge/discharge device 200, a power storage device 300, and a charging station 500.

**[0037]** The unauthorized connection detecting device 100 detects one of (i) whether or not a power storage device connectable to the charge/discharge device 200 is an unauthorized power storage device and (ii) whether or not a charge/discharge device connected to the power storage device 300 is an unauthorized charge/discharge device. It is noted that the unauthorized connection detecting device 100 may be either a general-purpose computer or a computer especially for detecting the unauthorized charge/discharge device or the unauthorized power storage device. The unauthorized connection detecting device 100 shall be detailed later.

**[0038]** The charge/discharge device 200 is connected with a power storage device, such as the power storage device 300, and charges or discharges the power storage device with power. Here, the charge/discharge device 200 is an authentic one and could be connected with an unauthorized power storage device. Furthermore, the charge/discharge device 200 is connected to a distribution board in a house 400, and supplies power to a load for use in the house 400 and receives power from the house 400.

**[0039]** In addition, the charge/discharge device 200 is connected to the unauthorized connection detecting device 100 via the house 400 and a communications net-

work 600. The charge/discharge device 200 can transmit the information held in itself to the unauthorized connection detecting device 100. The charge/discharge device 200 shall be detailed later.

**[0040]** The power storage device 300 is connected to a charge/discharge device, such as the charge/discharge device 200. The power storage device 300 receives power from and discharges power to the charge/discharge device 200. Here, the power storage device 300 is an authentic one and could be connected to an unauthorized charge/discharge device. In the embodiment, the power storage device 300 is an electric vehicle including a secondary battery such as a lithium-ion secondary battery; however, the power storage device 300 shall not be limited to an electric vehicle.

**[0041]** When connected to the charging station 500, the power storage device 300 can be charged by the charging station 500 with power. Here, when connected to the charging station 500, the power storage device 300 is connected to the unauthorized connection detecting device 100 via the charging station 500 and the communications network 600. Then, the power storage device 300 can transmit the information held in itself to the unauthorized connection detecting device 100. The power storage device 300 shall be detailed later.

**[0042]** The charging station 500 is a facility to charge a power storage device, such as the power storage device 300, with power. Moreover, following an instruction of the unauthorized connection detecting device 100, the charging station 500 transmits the information held in the power storage device 300 to the unauthorized connection detecting device 100.

**[0043]** Described next is a detailed structure of the unauthorized connection detecting device 100.

**[0044]** FIG. 2 depicts a block diagram showing a functional structure of the unauthorized connection detecting device 100 according to the embodiment.

**[0045]** As shown in FIG. 2, the unauthorized connection detecting device 100 includes a communications unit 110, an unauthorization detecting unit 120, a control unit 130, and a storage unit 140. Moreover, the storage unit 140 stores secret key data 141, a public key certificate 142, first charge/discharge information 143, and second charge/discharge information 144.

**[0046]** Through the communications network 600, the communications unit 110 transmits and receives information to and from the charge/discharge device 200 connected to the house 400 or the power storage device 300 connected to the charging station 500. Specifically, the communications unit 110 receives the first charge/discharge information in which first identification information and first connection information are associated each other. In other words, the communications unit 110 receives the later-described first charge/discharge information 273 from the charge/discharge device 200 via the communications network 600 with which the charge/discharge device 200 is connected. Then, the first charge/discharge information 273 received by the communications unit 110 is stored by the control unit 130 in the first charge/discharge information 143 in the storage unit 140.

**[0047]** FIG. 3 exemplifies the first charge/discharge information 143 according to the embodiment.

**[0048]** As shown in FIG. 3, the first charge/discharge information 143 is an information group in which the first identification information and the first connection information are associated each other.

**[0049]** Here, the first identification information is information for identifying an encryption key of a power storage device used for mutual authentication between the charge/discharge device 200 and the power storage device connectable to the charge/discharge device 200. Specifically, in the embodiment, the first identification information is ID information of a public key certificate, so that the ID information is used for identifying the public key certificate of a power storage device connectable to the charge/discharge device 200.

**[0050]** Furthermore, the first connection information is information on a power storage device and obtained when the power storage device is connected to the charge/discharge device 200. Specifically, the first connection information includes information indicating a time and a position when and where the power storage device was charged or discharged. In other words, the communications unit 110 receives the first charge/discharge information 273 in which the first identification information and the first connection information are associated each other. Here, the first connection information includes information indicating a time and a position when and where a power storage device was charged or discharged.

**[0051]** More specifically, the first connection information includes (i) time information indicating a time at which the charge/discharge device 200 charged or discharged the power storage device and (ii) position information indicating where the charge/discharge device 200 was. Here the position information may be, for example, GPS information of the charge/discharge device 200. It is noted that, in the case where address information of the charge/discharge device 200 is previously registered in the unauthorized connection detecting device 100, the position information may be the ID information of the charge/discharge device 200 to identify the charge/discharge device 200.

**[0052]** Hence, the communications unit 110 receives from the charge/discharge device 200 the first charge/discharge information 273 in which the first identification information, the time information, and the position information are associated one another. Here, the time information indicates a time when the charge/discharge device 200 charged or discharged a power storage device, and the position information indicates a position where the charge/discharge device 200 was. Then, the first charge/discharge information 273 is stored by the control unit 130 on the first charge/discharge information 143 in the storage unit 140.

**[0053]** As shown in FIG. 2, the communications unit 110 receives the second charge/discharge information in which second identification information and second connection information are associated each other. Specifically, when the power storage device 300 is connected to the charging station 500, the communications unit 110 receives the after-described second charge/discharge information 373 from the power storage device 300 via the communications network 600. Then, the second charge/discharge information 373 received by the communications unit 110 is stored by the control unit 130 on the second charge/discharge information 144 in the storage unit 140.

**[0054]** FIG. 4 exemplifies the second charge/discharge information 144 according to the embodiment.

**[0055]** As shown in FIG. 4, the second charge/discharge information 144 is an information group in which the second identification information and the second connection information are associated each other.

**[0056]** Here, the second identification information is information for identifying the encryption key of a charge/discharge device used for mutual authentication between the power storage device 300 and the charge/discharge device connectable with the power storage device 300. Specifically, in the embodiment, the second identification information is ID information of a public key certificate, so that the ID information is used for identifying the public key certificate of a charge/discharge device connectable to the power storage device 300.

**[0057]** Furthermore, the second connection information is information on a charge/discharge device and obtained when charge/discharge device is connected with the power storage device 300. Specifically, the second connection information includes charge/discharge device identification information for identifying the charge/discharge device and power storage device identification information for identifying the power storage device 300 connected to the charge/discharge device.

**[0058]** Here, the charge/discharge device identification information is position information, such as GPS information indicating the position of the charge/discharge device. It is noted that the charge/discharge device identification information may be position information, such as GPS information, indicating the position of the power storage device 300 obtained when the power storage device 300 was connected to a charge/discharge device.

**[0059]** Moreover, the charge/discharge device identification information shall not be limited to the above-described position information; instead, the charge/discharge device identification information may be, for example, direct current information which can identify a charge/discharge device. In other words, a direct current provided from a charge/discharge device has fluctuation which is unique to the charge/discharge device itself. Through the analysis of the fluctuation using a phase sample of the direct current, the charge/discharge device identification information can identify a charge/discharge device.

**[0060]** Furthermore, the power storage device identification information is, for example, ID information on a power storage device for identifying the power storage device 300. It is noted that any information may be used as the power storage device identification information as far as the information can identify the power storage device. The information includes ID information of a public key certificate, so that the ID information is used for identifying the public key certificate of the power storage device 300.

**[0061]** Hence, the communications unit 110 receives the second charge/discharge information 373 from the power storage device 300. Here, the second charge/discharge information 373 associates the second identification information with the second connection information that includes (i) the charge/discharge device identification information for identifying a charge/discharge device and (ii) the power storage device identification information for identifying the power storage device 300 connected to the charge/discharge device. Then, the second charge/discharge information 373 received by the communications unit 110 is stored by the control unit 130 on the second charge/discharge information 144 in the storage unit 140.

**[0062]** As shown in FIG. 2, the unauthorization detecting unit 120 detects whether or not a power storage device connected to the charge/discharge device 200 is an unauthorized power storage device by determining, using the first identification information and the first connection information included in the first charge/discharge information received by the communications unit 110, whether or not two or more power storage devices associated with a single first identification information item are present. In other words, the unauthorization detecting unit 120 reads through the control unit 130 the first charge/discharge information 143 stored in the storage unit 140, and performs the above detection.

**[0063]** Specifically, the unauthorization detecting unit 120 detects whether or not a power storage device connected to the charge/discharge device 200 is-an unauthorized power storage device, by determining, based on a relationship between times and positions included in a first connection information item associated with a single first identification information item, whether or not two or more power storage devices associated with the single first identification information item are present. Here, the first connection information item is included in the first connection information, and the first connection information item and the single first identification information item are included in the first charge/discharge information.

**[0064]** In addition, the unauthorization detecting unit 120 detects whether or not a charge/discharge device connected with the power storage device 300 is an unauthorized charge/discharge device, by determining, using the second identification information and the second connection information included in the second charge/discharge information received by the communi-

cations unit 110, whether or not two or more charge/discharge devices associated with a single second identification information item are present. In other words, the unauthorization detecting unit 120 reads through the control unit 130 the second charge/discharge information 144 stored in the storage unit 140, and performs the above detection.

**[0065]** Specifically, the unauthorization detecting unit 120 detects whether or not the charge/discharge device connected with the power storage device 300 is an unauthorized charge/discharge device, by determining whether or not two or more charge/discharge device identification information items, included in a second connection information item associated with a single second identification information item, indicate mutually different charge/discharge devices, thereby determining whether or not two or more charge/discharge devices associated with the single second identification information item are present. Here, the two or more charge/discharge device identification information items are included in the charge/discharge device identification information, the second connection information item is included in the second connection information, and the second connection information item and the single second identification item are included in the second charge/discharge information.

**[0066]** To be more specific, the unauthorization detecting unit 120 detects whether or not the charge/discharge device connected with the power storage device 300 is an unauthorized charge/discharge device, by determining whether or not two or more position information items, included in a second connection information item associated with a single second identification information item, indicate mutually different positions, thereby determining whether or not two or more charge/discharge devices associated with the single second identification information item are present. Here, the two or more position information items are included in the position information, the second connection information item is included in the second connection information, and the second connection information item and the single second identification information item are included in the single second identification information.

**[0067]** Moreover, the unauthorization detecting unit 120 detects whether or not the charge/discharge device connected with the power storage device 300 is an unauthorized charge/discharge device, by determining whether or not the number of the power storage devices 300, identified by two or more power storage device identification information items included in a second connection information item associated with a single second identification information item, is larger than or equal to a predetermined threshold, thereby determining whether or not two or more charge/discharge devices associated with the single second identification information item are present. Here, the two or more power storage device identification information items are included in the power storage device identification information, the second connection information item is included in the second connection information, and the second-connection information item and the single second identification information item are included in the second charge/discharge information

**[0068]** The control unit 130 gives an instruction to and controls the communications unit 110 and the unauthorization detecting unit 120.

**[0069]** For example, the control unit 130 (i) writes, in the first charge/discharge information 143 in the storage unit 140, the first charge/discharge information 273 received by the communications unit 110 from the charge/discharge device 200, and (ii) writes, in the second charge/discharge information 144 in the storage unit 140, the second charge/discharge information 373 received by the communications unit 110 from the power storage device 300.

**[0070]** In addition, the control unit 130 reads the first charge/discharge information 143 or the second charge/discharge information 144 stored in the storage unit 140, and provides the read first charge/discharge information 143 or the second charge/discharge information 144 to the unauthorization detecting unit 120.

**[0071]** Furthermore, the control unit 130 is also capable of creating a list of cryptographic modules of an unauthorized power storage device or an unauthorized charge/discharge device detected by the unauthorization detecting unit 120.

**[0072]** It is noted that the secret key data 141 and the public key certificate 142 stored in the storage unit 140 are used for mutual authentication when the communications unit 110 receives information from the charge/discharge device 200 or the power storage device 300.

**[0073]** Described next is a detailed structure of the charge/discharge device 200.

**[0074]** FIG. 5 depicts a block diagram showing a functional structure of the charge/discharge device 200 according to the embodiment.

**[0075]** As shown in FIG. 5, the charge/discharge device 200 includes a communications unit 210, a certificate information obtaining unit 220, a certificate verification unit 230, a time information detecting unit 240, a position information detecting unit 250, a control unit 260, and a storage unit 270. Moreover, the storage unit 270 stores secret key data 271, a public key certificate 272, and first charge/discharge information 273.

**[0076]** The communications unit 210 transmits and receives information to and from one of the unauthorized connection detecting device 100 and a power storage device. Specifically, the communications unit 210 transmits the first charge/discharge information 273 that is stored in the storage unit 270 to the unauthorized connection detecting device 100 via the house 400 and the communications network 600.

**[0077]** Here, the first charge/discharge information 273 is created when the power storage device is connected to the charge/discharge device 200. Similar to the first charge/discharge information 143 shown in FIG. 3, the

first charge/discharge information 273 is an information group in which the first identification information and the first connection information (time information and position information) are associated each other.

**[0078]** The first identification information is ID information of a public key certificate, so that the ID information is used for identifying the public key certificate of the power storage device connected to the charge/discharge device 200. The first identification information is obtained by the certificate information obtaining unit 220 when the power storage device is connected to the charge/discharge device 200. In other words, the certificate information obtaining unit 220 obtains the ID information of the public key certificate from the power storage device via the communications unit 210 when the power storage device is connected to the charge/discharge device 200, and stores the information in the first charge/discharge information 273 in the storage unit 270.

**[0079]** In addition, the time information in the first connection information indicates a time when the charge/discharge device 200 charged or discharged the power storage device. The time information is obtained by the time information detecting unit 240 when the power storage device is connected to the charge/discharge device 200. In other words, the time information detecting unit 240 obtains the time information when the power storage device is connected to the charge/discharge device 200, and stores the information in the first charge/discharge information 273 in the storage unit 270.

**[0080]** Moreover, the position information in the first connection information includes GPS information indicating the position of the charge/discharge device 200. The position information is obtained by the position information detecting unit 250 when the power storage device is connected to the charge/discharge device 200. In other words, the position information detecting unit 250 obtains the position information when the power storage device is connected to the charge/discharge device 200, and stores the information in the first charge/discharge information 273 in the storage unit 270.

**[0081]** It is noted that in the case where address information of the charge/discharge device 200 is previously registered in the unauthorized connection detecting device 100, the position information may be the ID information of the charge/discharge device 200 for identifying the charge/discharge device 200. Here, the ID information of the charge/discharge device 200 is obtained by the position information detecting unit 250 when the power storage device is connected to the charge/discharge device 200.

**[0082]** When a power storage device is connected to the charge/discharge device 200, the certificate verification unit 230 performs mutual authentication between the power storage device and the charge/discharge device 200 using the secret key data 271 and the public key certificate 272 stored in the storage unit 270. A specific description of how the certificate verification unit 230 performs the mutual authentication shall be described later.

**[0083]** The control unit 260 controls the communications unit 210, the certificate information obtaining unit 220, the certificate verification unit 230, the time information detecting unit 240, and the position information detecting unit 250.

**[0084]** Specifically, when a power storage device is connected to the charge/discharge device 200, the control unit 260 causes the certificate information obtaining unit 220 to obtain first identification information, the time information detecting unit 240 to obtain time information, and the position information detecting unit 250 to obtain position information. Then, the control unit 260 stores the obtained information in the first charge/discharge information 273 in the storage unit 270. In addition, the control unit 260 causes the communications unit 210 to read the first charge/discharge information 273 from the storage unit 270 and to transmit the read first charge/discharge information 273 to the unauthorized connection detecting device 100.

**[0085]** Moreover, when a power storage device is connected to the charge/discharge device 200, the control unit 260 causes the certificate verification unit 230 to perform, via the communications unit 210, mutual authentication between the power storage device and the charge/discharge device 200.

**[0086]** Described next is a detailed structure of the power storage device 300.

**[0087]** FIG. 6 depicts a block diagram showing a functional structure of the power storage device 300 according to the embodiment.

**[0088]** As shown in FIG. 6, the power storage device 300 includes a communications unit 310, a certificate information obtaining unit 320, a certificate verification unit 330, a charge/discharge device identification information obtaining unit 340, a power storage device identification information obtaining unit 350, a control unit 360, and a storage unit 370. Moreover, the storage unit 370 stores a secret key data 371, a public key certificate 372, and the second charge/discharge information 373.

**[0089]** The communications unit 310 transmits and receives information to and from one of the unauthorized connection detecting device 100 and a charge/discharge device power storage device. Specifically, the communications unit 310 transmits the second charge/discharge information 373, which is stored in the storage unit 370, to the unauthorized connection detecting device 100 via the charging station 500 and the communications network 600.

**[0090]** Here, the second charge/discharge information 373 is created when the power storage device 300 is connected to the charge/discharge device. Similar to the second charge/discharge information 144 shown in FIG. 4, the second charge/discharge information 373 is a group of information in which the second identification information and the second connection information (the charge/discharge device identification information and the power storage device identification information) are associated each other.

**[0091]** The second identification information is ID information of a public key certificate, so that the ID information is used for identifying the public key certificate of the charge/discharge device connected with the power storage device 300. The first identification information is obtained by the certificate information obtaining unit 320 when the charge/discharge device is connected to the power storage device 300. In other words, the certificate information obtaining unit 320 obtains the ID information of the public key certificate from the charge/discharge device via the communications unit 310 when the charge/discharge device is connected to the power storage device 300, and stores the information in the second charge/discharge information 373 in the storage unit 370.

**[0092]** Moreover, the charge/discharge device identification information in the second connection information is, for example, capable of identifying a charge/discharge device, such as GPS information indicating a position of the charge/discharge device. The charge/discharge device identification information is obtained by the power storage device identification information obtaining unit 350 when the charge/discharge device is connected to the power storage device 300. In other words, the power storage device identification information obtaining unit 350 obtains the charge/discharge device identification information when the charge/discharge device is connected to the power storage device 300, and stores the information in the second charge/discharge information 373 in the storage unit 370.

**[0093]** In addition, the power storage device identification information in the second connection information is, for example, capable of identifying a power storage device 300, such as ID information for identifying the power storage device 300. The power storage device identification information is obtained by the charge/discharge device identification information obtaining unit 340 when the charge/discharge device is connected with the power storage device 300. In other words, the charge/discharge device identification information obtaining unit 340 obtains the charge/discharge device identification information when the charge/discharge device is connected with the power storage device 300, and stores the information in the second charge/discharge information 373 in the storage unit 370.

**[0094]** When a charge/discharge device is connected with the power storage device 300, the certificate verification unit 330 performs mutual authentication between the charge/discharge device and the power storage device 300 using the secret key data 371 and the public key certificate 372 stored in the storage unit 370. A specific description of how the certificate verification unit 330 performs the mutual authentication shall be described later.

**[0095]** The control unit 360 controls the communications unit 310, the certificate information obtaining unit 320, the certificate verification unit 330, the charge/discharge device identification information obtaining unit 340, and the power storage device identification information obtaining unit 350.

**[0096]** Specifically, when a charge/discharge device is connected with the power storage device 300, the control unit 360 causes the certificate information obtaining unit 320 to obtain second identification information, the charge/discharge device identification information obtaining unit 340 to obtain charge/discharge deice identification information, and the power storage device identification information obtaining unit 350 to obtain power storage device identification information. Then, the control unit 360 stores the information in the second charge/discharge information 373 in the storage unit 370. In addition, the control unit 360 causes the communications unit 310 to read the second charge/discharge information 373 from the storage unit 370 and to transmit the read second charge/discharge information 373 to the unauthorized connection detecting device 100.

**[0097]** Moreover, when a charge/discharge device is connected to the power storage device 300, the control unit 360 causes the certificate verification unit 330 to perform, via the communications unit 310, mutual authentication between the charge/discharge device and the power storage device 300.

**[0098]** Described next is processing performed by the charge/discharge device 200.

**[0099]** FIG. 7 depicts a flowchart exemplifying an operation performed by the charge/discharge device 200 according to the embodiment.

**[0100]** As shown in FIG. 7, the communications unit 210 first detects that a power storage device has been connected to the charge/discharge device 200 (S102). Here, the charge/discharge device 200 can be connected not only to an authentic power storage device 300 but also to an unauthorized power storage device.

**[0101]** Hence, the certificate verification unit 230 performs mutual authentication between the power storage device and the charge/discharge device 200, using the secret key data 271 and the public key certificate 272 stored in the storage unit 270 (S104). A specific description of how the certificate verification unit 230 performs the mutual authentication shall be described later.

**[0102]** Then, when the mutual authentication is properly performed, the processing proceeds to the next step. Here, even though the connected power storage device is an unauthorized one, the mutual authentication could be properly performed between the unauthorized power storage device and the charge/discharge device 200, in the case where a cryptographic module of the authentic power storage device 300 is analyzed in an unauthorized manner and the analyzed module is cloned and fraudulently introduced into the unauthorized power storage device.

**[0103]** Then, through the communications unit 210, the certificate information obtaining unit 220 obtains the first identification information from the power storage device connected to the charge/discharge device 200 (S106). Specifically, the certificate information obtaining unit 220 obtains ID information of the public key certificate of the

power storage device.

**[0104]** In addition, the time information detecting unit 240 obtains time information and the position information detecting unit 250 obtains position information, so that the charge/discharge device 200 obtains first connection information including the time information and the position information (S108). It is noted that, in the case where address information of the charge/discharge device 200 is previously registered in the unauthorized connection detecting device 100, the position information may be the ID information of the charge/discharge device 200 to identify the charge/discharge device 200. Here, the ID information of the charge/discharge device 200 may be obtained by the position information detecting unit 250 when the power storage device is connected to the charge/discharge device 200.

**[0105]** Then, the control unit 260 stores in the first charge/discharge information 273 in the storage unit 270 the first identification information and the first connection information obtained by the communications unit 210, the certificate information obtaining unit 220, and the time information detecting unit 240 (S110).

**[0106]** Then, the control unit 260 determines whether or not the communications unit 210 can transmit (upload) the first charge/discharge information 273 to the unauthorized connection detecting device 100 (S112). For example, when the charge/discharge device 200 is connected to the unauthorized connection detecting device 100 via the communications network 600, the control unit 260 determines that the communications unit 210 can upload the first charge/discharge information 273 to the unauthorized connection detecting device 100.

**[0107]** Then, in the case where the determination result shows that the communications unit 210 can upload, the first charge/discharge information 273 to the unauthorized connection detecting device 100 (S112: Y), the control unit 260 causes the communications unit 210 to read the first charge/discharge information 273 from the storage unit 270, and to transmit the read first charge/discharge information 273 to the unauthorized connection detecting device 100 (S114).

**[0108]** In the case where the determination result shows that the communications unit 210 cannot upload the first charge/discharge information 273 to the unauthorized connection detecting device 100 (S112: N), the control unit 260 finishes processing.

**[0109]** It is noted that the control unit 260 may wait until the communications unit 210 is ready to upload the first charge/discharge information 273 to the unauthorized connection detecting device 100. Upon determining that the communications unit 210 is ready for the upload, the control unit 260 may cause the communications unit 210 to transmit the first charge/discharge information 273 to the unauthorized connection detecting device 100.

**[0110]** Alternatively, the control unit 260 may wait until a predetermined amount of information is accumulated in the first charge/discharge information 273. Then, the control unit 260 may cause the communications unit 210 to transmit the first charge/discharge information 273 to the unauthorized connection detecting device 100.

**[0111]** Hence, the processing performed by the charge/discharge device 200 ends.

**[0112]** Described next is processing performed by the power storage device 300.

**[0113]** FIG. 8 depicts a flowchart exemplifying an operation performed by the power storage device 300 according to the embodiment.

**[0114]** As shown in FIG. 8, the communications unit 310 first detects that a charge/discharge device has been connected to the power storage device 300 (S202). Here, the power storage device 300 can be connected not only to an authentic charge/discharge device 200 but also to an unauthorized charge/discharge device.

**[0115]** Then, the certificate verification unit 330 performs mutual authentication between the power storage device 300 and the connected charge/discharge device, using the secret key data 371 and the public key certificate 372 stored in the storage unit 370 (S204). A specific description of how the certificate verification unit 330 performs the mutual authentication shall be described later.

**[0116]** Then, when the mutual authentication is properly performed, the processing proceeds to the next step. Here, even though the connected charge/discharge device is an unauthorized one, the mutual authentication could be properly performed between the unauthorized connected charge/discharge device and the power storage device 300, in the case where a cryptographic module of the authentic charge/discharge device 200 is analyzed in an unauthorized manner and the analyzed module is cloned and fraudulently introduced into the unauthorized charge/discharge device.

**[0117]** Then, through the communications unit 310, the certificate information obtaining unit 320 obtains the second identification information from the charge/discharge device connected with the power storage device 300 (S206). Specifically, the certificate information obtaining unit 320 obtains ID information of the public key certificate of the power storage device.

**[0118]** In addition, the charge/discharge device identification information obtaining unit 340 obtains charge/discharge device identification information and the power storage device identification information obtaining unit 350 obtains power storage device identification information, so that the power storage device 300 obtains second connection information including the charge/discharge device identification information and the power storage device identification information (S208).

**[0119]** Then, the control unit 360 stores in the first charge/discharge information 373 in the storage unit 370 the second identification information and the second connection information obtained by the communications unit 310, the certificate information obtaining unit 320, and the charge/discharge device identification information obtaining unit 340 (S210).

**[0120]** Then, the control unit 360 determines whether

or not the communications unit 310 can transmit (upload) the second charge/discharge information 373 to the unauthorized connection detecting device 100 (S212). For example, when the power storage device 300 is connected to the charging station 500, the power storage device 300 is connected to the unauthorized connection detecting device 100 via the communications network 600. Hence, the control unit 360 determines that the communications unit 310 can upload the second charge/discharge information 373 to the unauthorized connection detecting device 100.

**[0121]** Then, in the case where the determination result shows that the communications unit 310 can upload the second charge/discharge information 373 to the unauthorized connection detecting device 100 (S212: Y), the control unit 360 causes the communications unit 310 to read the second charge/discharge information 373 from the storage unit 370, and to transmit the read second charge/discharge information 373 to the unauthorized connection detecting device 100 (S214).

**[0122]** In the case where the determination result shows that the communications unit 310 cannot upload the second charge/discharge information 373 to the unauthorized connection detecting device 100 (S212: N), the control unit 360 finishes processing.

**[0123]** It is noted that the control unit 360 may wait until the communications unit 310 is ready to upload the second charge/discharge information 373 to the unauthorized connection detecting device 100. Upon determining that the communications unit 310 is ready for the upload, the control unit 360 may cause the communications unit 310 to transmit the second charge/discharge information 373 to the unauthorized connection detecting device 100.

**[0124]** Alternatively, the control unit 360 may wait until a predetermined amount of information is accumulated in the second charge/discharge information 373. Then, the control unit 360 may cause the communications unit 310 to transmit the second charge/discharge information 373 to the unauthorized connection detecting device 100.

**[0125]** Hence, the processing performed by the power storage device 300 ends.

**[0126]** Next, described in detail is mutual authentication processing (S104 in FIG. 7 and S204 in FIG. 8) performed by a charge/discharge device and a power storage unit. It is noted that the mutual authentication processing is performed (i) by an authentic charge/discharge device 200 and one of an authentic power storage unit and an unauthorized power storage unit, and (ii) by an authentic power storage device 300 and one of an authentic charge/discharge device and an unauthorized charge/discharge device. In the processing below, the mutual authentication is performed by the charge/discharge device 200 and the power storage device 300 for the sake of simplicity.

**[0127]** FIG. 9 depicts a flowchart exemplifying mutual authentication processing performed by the charge/discharge device 200 and the power storage device 300 according to the embodiment.

**[0128]** As shown in FIG. 9, the certificate verification unit 230 in the charge/discharge device 200 first transmits the public key certificate 272 stored in the storage unit 270 to the certificate verification unit 330 in the power storage device 300 (S302). Furthermore, the certificate verification unit 330 transmits the public key certificate 372 stored in the storage unit 370 to the certificate verification unit 230 (S304).

**[0129]** Then, the certificate verification unit 230 checks the received certificate (S306). In the case where the certificate is invalid (S310: N), the processing ends. In the case where the certificate is valid (S310: Y), the processing proceeds to the next step.

**[0130]** Moreover, the certificate verification unit 330 also checks the received certificate (S308). In the case where the certificate is invalid (S312: N), the processing ends. In the case where the certificate is valid (S312: Y), the processing proceeds to the next step.

**[0131]** Then, the certificate verification unit 330 creates a random number r1, and transmits the random number r1 to the certificate verification unit 230 (S314). Then, the certificate verification unit 230 receives the random number r1. In response to the random number r1, the certificate verification unit 230 creates a signature Sig(r1) using a secret key SKs described in the secret key data 271, and a random number r2.

**[0132]** Next, the certificate verification unit 230 transmits the random number r2 and the signature Sig(r1) to the certificate verification unit 330 (S316). Then, the certificate verification unit 330 receives the random number r2 and the signature Sig(r1), and checks the signature Sig(r1) using a public key described in the public key certificate 272.

**[0133]** In the case where the certificate verification unit 330 determines that the signature Sig(r1) is valid, the certificate verification unit 330 creates, in response to the random number r2, a signature Sig(r2) using a secret key SK_i described in the secret key data 371. Then, the certificate verification unit 330 transmits the signature Sig(r2) to the certificate verification unit 230 (S318). In the case where the certificate verification unit 330 determines that the signature Sig(r1) is invalid, the certificate verification unit 330 returns NG to the certificate verification unit 230, and breaks off the connections with the charge/discharge device 200.

**[0134]** Then, the certificate verification unit 230 receives the signature Sig(r2), and checks the signature Sig(r2) using a public key described in the public key certificate 372.

**[0135]** Then, in the case where the certificate verification unit 230 determines that the signature Sig(r2) is valid, the certificate verification unit 230 returns OK to the certificate verification unit 330 (S320). In the case where the certificate verification unit 230 determines that the signature Sig(r2) is invalid, the certificate verification unit 230 returns NG to the certificate verification unit 330, and breaks off the connections with the charge/discharge device 300.

**[0136]** Hence, the mutual authentication processing (S104 in FIG. 7 and S204 in FIG. 8) performed by the charge/discharge device and the power storage unit ends.

**[0137]** Described next is how the unauthorized connection detecting device 100 detects an unauthorized power storage device.

**[0138]** FIG. 10 depicts a flowchart exemplifying an operation of how the unauthorized connection detecting device 100 according to the embodiment detects an unauthorized power storage device.

**[0139]** As shown in FIG. 10, the communications unit 110 first receives the first charge/discharge information 273 from the charge/discharge device 200 via the communications network 600 (S402). Then, the first charge/discharge information 273 received by the communications unit 110 is stored by the control unit 130 in the first charge/discharge information 143 in the storage unit 140 (S402).

**[0140]** Here, in the case where the charge/discharge device 200 is connected with an authentic power storage apparatus, the communications unit 110 receives first charge/discharge information 273 corresponding to the authentic power storage apparatus. In the case where the charge/discharge device 200 is connected with an unauthorized power storage device, the communications unit 110 receives first charge/discharge information 273 corresponding to the unauthorized power storage device.

**[0141]** Then, using the first identification information and the first connection information included in the first charge/discharge information received by the communications unit 110, the unauthorization detecting unit 120 determines whether or not two or more power storage devices associated with a single first identification information item are present (S404).

**[0142]** In the case where the determination result shows that two or more power storage devices associated with a single first identification information item are present (S404: Y), the unauthorization detecting unit 120 detects that the power storage device connected to the charge/discharge device 200 is an unauthorized one (S406). In other words, the unauthorization detecting unit 120 reads the first charge/discharge information 143 stored in the storage unit 140 to perform the above detection.

**[0143]** Specifically, the unauthorization detecting unit 120 detects whether or not the power storage device connected to the charge/discharge device 200 is an unauthorized power storage device, by determining, based on a relationship between times and positions included in a first connection information item associated with a single first identification information item, whether or not two or more power storage devices associated with the single first identification information item are present. Here, the first connection information item is included in the first connection information, and the first connection information item and the single first identification information item are included in the first charge/discharge information.

**[0144]** For example, the unauthorization detecting unit 120 determines whether or not an unnatural relationship is found between the times and positions (i) included in the first connection information and (ii) associated with a single first identification information item, and determines whether or not two or more power storage devices associated with the single first identification information are present. Here, the unnatural relationship is the case where, for example, a power storage device cannot possibly travel a distance between the positions within a time period between the times. Based on a previously prepared database table, the unauthorization detecting unit 120 can determine whether or not the relationship is unnatural.

**[0145]** It is noted that, in the case where the address information of the charge/discharge device 200 and the ID information of the charge/discharge device 200 for identifying the charge/discharge device 200 are associated each other and previously registered in the unauthorized connection detecting device 100, the information on the positions may be the ID information of the charge/discharge device 200.

**[0146]** Then, the control unit 130 creates a list of cryptographic modules of unauthorized power storage devices detected by the unauthorization detecting unit 120, and stores the list in the storage unit 140.

**[0147]** In the case where the determination result shows that no other power storage device associated with a single first identification information is present (S404: N), the unauthorization detecting unit 120 determines that the power storage device is not an unauthorized one and finishes the processing.

**[0148]** Hence, the unauthorized connection detecting device 100 finishes the processing for detecting an unauthorized power storage device.

**[0149]** Described next is how the unauthorized connection detecting device 100 detects an unauthorized charge/discharge device.

**[0150]** FIG. 11 depicts a flowchart exemplifying an operation of how the unauthorized connection detecting device 100 according to the embodiment detects an unauthorized charge/discharge device.

**[0151]** As shown in FIG. 11, the communications unit 110 first receives the second charge/discharge information 373 from the power storage device 300 via the communications network 600 (S502). Then, the second charge/discharge information 373 received by the communications unit 110 is stored by the control unit 130 in the second charge/discharge information 144 in the storage unit 140 (S502).

**[0152]** Here, in the case where the power storage device 300 is connected to an authentic power storage apparatus, the communications unit 110 receives second charge/discharge information 373 corresponding to the authentic power storage apparatus. In the case where the power storage device 300 is connected to an unauthorized power storage device, the communications unit 110 receives second charge/discharge information 373

corresponding to the unauthorized power storage device.

**[0153]** Then, using the second identification information and the second connection information included in the second charge/discharge information received by the communications unit 110, the unauthorization detecting unit 120 determines whether or not two or more charge/discharge devices associated with a single second identification information item are present (S504).

**[0154]** Then, in the case where the determination result shows that two or more charge/discharge device associated with the single second identification information item are present (S504: Y), the unauthorization detecting unit 120 detects that the charge/discharge device connected with the power storage device 300 is an unauthorized one (S506). In other words, the unauthorization detecting unit 120 reads the second charge/discharge information 144 stored in the storage unit 140 to perform the above detection.

**[0155]** Specifically, the unauthorization detecting unit 120 detects whether or not a charge/discharge device connected with the power storage device 300 is an unauthorized charge/discharge device, by determining whether or not two or more charge/discharge device identification information items, included in a second connection information associated with a single second identification information item, indicate mutually different charge/discharge devices, and thereby determining whether or not two or more charge/discharge devices associated with the single second identification information item are present. Here, the two or more charge/discharge device identification information items are included in the charge/discharge device identification information, the second connection information item is included in the second connection information, and the second connection information item and the single second identification item are included in the second charge/discharge information.

**[0156]** To be more specific, the unauthorization detecting unit 120 detects whether or not a charge/discharge device connected with the power storage device 300 is an unauthorized charge/discharge device, by determining whether or not two or more position information items, included in a second connection information item associated with a single second identification information item, indicate mutually different positions, thereby determining whether or not two or more charge/discharge devices associated with the single second identification information item are present. Here, the two or more position information items are included in the position information, the second connection information item is included in the second connection information, and the second connection information item and the single second identification information item are included in the single second identification information.

**[0157]** It is noted that the position information items can indicate different positions each other because the owner of the charge/discharge device has moved to a new address. In this case, the unauthorization detecting unit 120 obtains information showing that the charge/discharge device has moved to accurately determine whether or not two or more charge/discharge devices associated with the above single identification information item are present.

**[0158]** Moreover, the unauthorization detecting unit 120 may detect whether or not a charge/discharge device connected with the power storage device 300 is an unauthorized charge/discharge device by determining whether or not the number of the power storage devices 300, identified by two or more power storage device identification information items included in a second connection information item associated with a single second identification information item, is larger than or equal to a predetermined threshold, thereby determining whether or not two or more charge/discharge devices associated with the single second identification information item are present. Here, the two or more power storage device identification information items are included in the power storage device identification information, the second connection information item is included in the second connection information, and the second connection information item and the single second identification information item are included in the second charge/discharge information

**[0159]** Here, the unauthorization detecting unit 120 may change the above threshold, depending on the kind of a charge/discharge device. In other words, in the case where the charge/discharge device is for a commercial facility or a charging station, the threshold of the unauthorization detecting unit 120 may be set higher than that of the charge/discharge device for the standard home.

**[0160]** Then, the control unit 130 creates a list of cryptographic modules of unauthorized charge/discharge devices detected by the unauthorization detecting unit 120, and stores the list in the storage unit 140.

**[0161]** In the case where the determination result shows that no other charge/discharge device associated with a single second identification information is present (S504: N), the unauthorization detecting unit 120 determines that the charge/discharge device is not an unauthorized one and finishes the processing.

**[0162]** Hence, the unauthorized connection detecting device 100 finishes the processing for detecting an unauthorized charge/discharge device.

[Modification 1]

**[0163]** Described next is a modification of how the unauthorized connection detecting device 100 detects an unauthorized charge/discharge device.

**[0164]** FIG. 12 depicts a flowchart exemplifying an operation of how the unauthorized connection detecting device 100 according to Modification 1 of the embodiment detects an unauthorized charge/discharge device.

**[0165]** As shown in FIG. 12, the communications unit 110 first receives the second charge/discharge information 373 from the power storage device 300 via the com-

munications network 600 (S602). Then, the second charge/discharge information 373 received by the communications unit 110 is stored by the control unit 130 in the second charge/discharge information 144 in the storage unit 140 (S602).

**[0166]** Then, the unauthorization detecting unit 120 determines whether or not multiple position information items, included in the second connection information and associated with a single second identification information item included in the second charge/discharge information, indicate different positions each other (S604).

**[0167]** Then, in the case where the determination result shows that the multiple position information items indicate a single position (S604: N), the unauthorization detecting unit 120 determines whether or not the number of power storage devices 300 is larger than or equal to a predetermined threshold (S606). Here, the power storage devices 300 are identified by multiple power storage device identification information items (i) included in the second connection information and (ii) associated with a single second identification information item included in the second charge/discharge information.

**[0168]** Then, in the case where the determination result shows that the multiple position information items indicate different positions each other (S604: Y) or the number of power storage devices 300 identified by the multiple power storage device identification information items is larger than or equal to a predetermined threshold (S606: Y), the unauthorization detecting unit 120 detects that the charge/discharge device connected with the power storage device 300 is an unauthorized one (S608).

**[0169]** Then, the control unit 130 creates a list of cryptographic modules of unauthorized charge/discharge devices, and stores the list in the storage unit 140.

**[0170]** Furthermore, in the case where the determination result shows that the number of the power storage devices 300 identified by the multiple power storage device identification information items is smaller than the predetermined threshold (S606: N), the unauthorization detecting unit 120 determines that the charge/discharge device connected with the power storage device 300 is not an unauthorized one, and finishes the processing.

**[0171]** Here, the unauthorization detecting unit 120 may change the above threshold, depending on the kind of a charge/discharge device. In other words, in the case where the charge/discharge device is for a commercial facility or a charging station, the threshold of the unauthorization detecting unit 120 may be set higher than that of the charge/discharge device for the standard home.

**[0172]** Hence, the unauthorized connection detecting device 100 finishes the processing for detecting an unauthorized charge/discharge device.

[Modification 2]

**[0173]** In the above embodiment and Modification 1, the first identification information is information for identifying a public key certificate of a power storage device connectable to the charge/discharge device 200. In Modification 2, the first identification information is information for identifying a secret key of the power storage device. Moreover, in the above embodiment and Modification 1, the second identification information is information for identifying a public key certificate of a charge/discharge device connectable with the power storage device 300. In Modification 2, the second identification information is information for identifying a secret key of the charge/discharge device.

**[0174]** In other words, the charge/discharge device 200 stores in the storage unit 270 a list of information for identifying a secret key of a power storage device. With reference to the secret key list, the charge/discharge device 200 identifies the secret key of a power storage device connected to the charge/discharge device 200, and stores in the storage unit 270 the first charge/discharge information 273 using the information for identifying the secret key as the first identification information.

**[0175]** Similarly, the power storage device 300 stores in the storage unit 370 a list of information for identifying a secret key of a charge/discharge device. With reference to the secret key list, the power storage device 300 identifies the secret key of a charge/discharge device connected to the power storage device 300, and stores in the storage unit 370 the second charge/discharge information 373 using the information for identifying the secret key as the second identification information.

**[0176]** It is noted that when the unauthorized connection detecting device 100 holds the above secret key list, the charge/discharge device 200 or the power storage device 300 does not have to hold the secret key list. Instead, the charge/discharge device 200 or the power storage device 300 may obtain the list from the unauthorized connection detecting device 100 via the communications network 600. In other words, the charge/discharge device 200 or the power storage device 300 transmits the key ID of a secret key to the unauthorized connection detecting device 100, and obtains information for identifying the secret key. It is noted that, in this case, the unauthorized connection detecting device 100 can prevent an unauthorized connection by performing verification using the received secret key.

**[0177]** Next, described in detail is mutual authentication processing (S104 in FIG. 7 and S204 in FIG. 8) performed by a charge/discharge device and a power storage unit. It is noted that the mutual authentication processing is performed (i) by an authentic charge/discharge device 200 and one of an authentic power storage unit and an unauthorized power storage unit, and (ii) by an authentic power storage device 300 and one of an authentic charge/discharge device and an unauthorized charge/discharge device. In the processing below, the mutual authentication is performed by the charge/discharge device 200 and the power storage device 300 for the sake of simplicity.

**[0178]** FIG. 13 depicts a flowchart exemplifying mutual authentication processing performed by the charge/dis-

charge device 200 and the power storage device 300 according to Modification 2 of the embodiment.

**[0179]** As shown in FIG. 13, the charge/discharge device 200 first transmits a key ID (IDp_i); namely a secret key, to the power storage device 300 (S702). Moreover, the power storage device 300 transmits a key ID (IDv_i); namely a secret key, to the charge/discharge device 200 (S704).

**[0180]** Then, with reference to the secret key list stored in the storage unit 270, the charge/discharge device 200 searches for the secret key of the power storage device 300 (S706). With reference to the secret key list stored in the storage unit 370, the power storage device-300 searches for the secret key of the charge/discharge device 200 (S708).

**[0181]** Then, the power storage device 300 creates a random number r1, and transmits the random number r1 to the charge/discharge device 200 (S710). Then, the charge/discharge device 200 encrypts the received random number r1 with a secret key SKp_i, creates the random number r2, and transmits the encrypted random number r1 and the random number r2 (S712).

**[0182]** Then, the power storage device 300 receives the random number r2 and information created of the encrypted random number r1 with the secret key SKp_i, and checks whether the information matches the result of the encryption of the random number r1 with the secret key SKp_i.

**[0183]** Then, in the case where the power storage device 300 determines that the information matches the encryption result, the power storage device 300 encrypts the random number r2 with a secret key SKv_i and transmits the encrypted random number r2 to the charge/discharge device 200 (S714). It is noted that in the case where the information fails to match the encryption result, the power storage device 300 returns NG to the charge/discharge device 200, and breaks off the connections to the charge/discharge device 200.

**[0184]** Then, the charge/discharge device 200 receives the information created of the encrypted random number r2 with the secret key SKv_i, and checks whether the information matches the result of the encryption of the random number r2 with the secret key SKv_i.

**[0185]** Then, in the case where the charge/discharge device 200 determines that the information matches the encryption result, the charge/discharge device 200 returns OK to the power storage device 300 (S716). It is noted that in the case where the information fails to match the encryption result, the charge/discharge device 200 returns NG to the power storage device 300, and breaks off the connections to the power storage device 300.

**[0186]** Hence, the mutual authentication processing (S104 in FIG. 7 and S204 in FIG. 8) performed by the charge/discharge device and the power storage unit ends.

**[0187]** As described above, the unauthorized connection detecting device 100 according to the embodiment of the present invention and the modifications thereof detects whether or not a power storage device is an unauthorized power storage device by (i) receiving the first charge/discharge information in which the first identification information for identifying a secret key of a power storage device and the first connection information on a power storage device are associated each other, and (ii) determining, using the first charge/discharge information, whether or not two or more power storage devices associated with a single first identification information are present. Here, on authentic power storage devices, a single first identification information item is assigned to one power storage device. When a cryptographic module of an authentic product is introduced in an unauthorized manner, however, two or more power storage devices associated with a single first identification information item are to be present. Hence, in the case where two or more power storage devices associated with a single first identification information are present, the unauthorized connection detecting device 100 can determine that any one or more of the power storage devices are unauthorized ones. Thus, the unauthorized connection detecting device 100 can detect an unauthorized power storage device having a cryptographic module of an authentic product introduced in an unauthorized manner.

**[0188]** Furthermore, the unauthorized connection detecting device 100 detects whether or not a power storage device is an unauthorized power storage device by determining, based on a relationship between times and positions associated with a single first identification information item, whether or not two or more power storage devices associated with the single first identification information item are present. In other words, in the case where there is an unnatural relationship between times and positions associated with a single first identification information item, the unauthorized connection detecting device 100 determines that two or more power storage devices associated with the single first identification information item are present. For example, in the case where a power storage device cannot possibly travel a distance between two positions within a time period between two times when the two positions and the two times are associated with a single first identification information item, the unauthorized connection detecting device 100 determines that two or more power storage devices associated with the single first identification information item are present. Thus, the unauthorized connection detecting device 100 can detect an unauthorized power storage device having a cryptographic module of an authentic product introduced in an unauthorized manner.

**[0189]** In addition, information on a time included in the first charge/discharge information received by the unauthorized connection detecting device 100 is time information indicating the time at which a charge/discharge device charges or discharges a power storage device. Information on a position is position information such as GPS information indicating a position of the charge/discharge device. Since the above features allow the unauthorized connection detecting device 100 to receive eas-

ily created first charge/discharge information, the unauthorized connection detecting device 100 can easily detect an unauthorized power storage device having a cryptographic module of an authentic product introduced in an unauthorized manner.

**[0190]** In addition, the unauthorized connection detecting device 100 detects whether or not a charge/discharge device is an unauthorized charge/discharge device by receiving the second charge/discharge information in which the second identification information and the second connection information are associated each other, and (ii) determining, using the second charge/discharge information, whether or not two or more charge/discharge devices associated with a single second identification information item are present. The second identification information is information for identifying the encryption key of the charge/discharge device, and the second connection information is information on the charge/discharge device. Here, on authentic charge/discharge devices, a single second identification information item is assigned to one charge/discharge device. When a cryptographic module of an authentic product is introduced in an unauthorized manner, however, two or more charge/discharge devices associated with a single second identification information item are to be present. Hence, in the case where two or more charge/discharge devices associated with a single second identification information item are present, the unauthorized connection detecting device 100 can determine that any one or more of the power storage devices are unauthorized ones. Thus, the unauthorized connection detecting device 100 can detect an unauthorized charge/discharge device having a cryptographic module of an authentic product introduced in an unauthorized manner.

**[0191]** Furthermore, the unauthorized connection detecting device 100 detects whether or not a charge/discharge device is an unauthorized charge/discharge device, by determining whether or not two or more charge/discharge device identification information items associated with a single second identification information item indicate mutually different charge/discharge devices, thereby determining whether or not two or more charge/discharge devices associated with the single second identification information item are present. In other words, in the case where two or more charge/discharge device identification information items associated with a single second identification information item indicate different charge/discharge devices, the unauthorized connection detecting device 100 determines that two or more charge/discharge devices associated with the single second identification information item are present. Thus, the unauthorized connection detecting device 100 can detect an unauthorized charge/discharge device having a cryptographic module of an authentic product introduced in an unauthorized manner.

**[0192]** Moreover, the charge/discharge device identification information included in the second charge/discharge information received by the unauthorized connection detecting device 100 is position information indicating the position of a charge/discharge device. The unauthorized connection detecting device 100 detects whether or not a charge/discharge device is an unauthorized charge/discharge device by determining whether or not two or more position information items associated with a single second identification information item indicate different positions each other, thereby determining whether or not two or more charge/discharge devices associated with the single second identification information item are present. The two or more position information items are included in the position information. Here, the charge/discharge device is placed at a predetermined position, and never found at two or more sites. Hence, in the case where two or more position information items associated with a single second identification information item indicate different positions each other, the unauthorized connection detecting device 100 determines that two or more charge/discharge devices associated with the single second identification information item are present. Thus, the unauthorized connection detecting device 100 can detect an unauthorized charge/discharge device having a cryptographic module of an authentic product introduced in an unauthorized manner.

**[0193]** Furthermore, the charge/discharge device identification information included in the second charge/discharge information received by the unauthorized connection detecting device 100 may be direct current information indicating a fluctuation of a direct current provided from a charge/discharge device. The unauthorized connection detecting device 100 may detect whether or not a charge/discharge device is an unauthorized charge/discharge device, by determining whether or not two or more direct current information items associated with a single second identification information item indicate mutually different fluctuations, thereby determining whether or not two or more charge/discharge devices associated with the single second identification information item are present. The two or more direct current information items are included in the direct current information. Here, a direct current provided from a charge/discharge device has fluctuation which is unique to the charge/discharge device itself. Through the analysis of the fluctuation using a phase sample of the direct current, the charge/discharge device can be identified. Hence, in the case where two or more direct current information items associated with a single second identification information item indicate different fluctuations each other, the unauthorized connection detecting device 100 determines that two or more charge/discharge devices associated with the single second identification information item are present. Thus, the unauthorized connection detecting device 100 can detect an unauthorized charge/discharge device having a cryptographic module of an authentic product introduced in an unauthorized manner.

**[0194]** Moreover, the unauthorized connection detecting device 100 detects whether or not a charge/discharge

device is an unauthorized charge/discharge device by determining whether or not the number of power storage devices, identified by two or more power storage device identification information items associated with a single second identification information item, is larger than or equal to a predetermined threshold, thereby determining whether or not two or more charge/discharge devices associated with the single second identification information item are present. Here, the two or more power storage device identification information items being included in the power storage device identification information. Here, the number of power storage devices to be connected to one charge/discharge device is limited. In the case where the number of the connected power storage devices is larger than or equal to a predetermined threshold, two or more charge/discharge devices associated with a single second identification information item are to be present. In other words, in the case where the number of power storage devices associated with a single second identification information item is larger than or equal to a predetermined threshold, the unauthorized connection detecting device 100 determines that two or more charge/discharge devices associated with the single second identification information item are present. Thus, the unauthorized connection detecting device 100 can detect an unauthorized charge/discharge device having a cryptographic module of an authentic product introduced in an unauthorized manner.

**[0195]** Furthermore, the unauthorized connection detecting device 100 receives information via the communications network 600 connected either with the charging station 500 or a charge/discharge device. In other words, when a power storage device is either charged at the charging station 500 or one of charged and discharged by a charge/discharge device, the unauthorized connection detecting device 100 can easily receive the information. Thus, the unauthorized connection detecting device 100 can easily obtain information and detect an unauthorized charge/discharge device having a cryptographic module of an authentic product introduced in an unauthorized manner.

**[0196]** Although described in detail above is the unauthorized connection detecting device 100 according to an exemplary embodiment and modifications thereof, those skilled in the art will readily appreciate that various modifications may be made in the exemplary embodiment and the modifications without materially departing from the principles and spirit of the inventive concept, the scope of which is defined in the appended Claims and their equivalents. Moreover, constituent elements in the embodiment and the modifications may be combined each other.

**[0197]** For example, in the present embodiment and the modifications thereof, the unauthorized connection detecting system 10 includes both of the charge/discharge device 200 and the power storage device 300. However, the unauthorized connection detecting device 100 may have only one of the charge/discharge device 200 and the power storage device 300.

**[0198]** Moreover, the unauthorized connection detecting device 100 does not have to include all the constituent features shown in FIG. 2. FIG. 14 depicts a block diagram showing a minimal structure of the unauthorized connection detecting device according to the embodiment and Modifications thereof. As shown in FIG. 14, an unauthorized connection detecting device 101 includes at least the communications unit 110 and the unauthorization detecting unit 120. Such a structure makes it possible to achieve an effect similar to that of the unauthorized connection detecting device 100 according to the embodiment and the modifications thereof.

**[0199]** In addition, the present invention can be implemented in the form of an unauthorized connection detecting method including characteristic processing to be carried out by the unauthorized connection detecting device or the unauthorized connection detecting system as steps. Moreover, the steps included in the unauthorized connection detecting method may be implemented in the form of a program to be executed by a computer and a computer-readable recording medium in which the program is stored. As a matter of course, the program may be distributed via a recording medium such as a CD-ROM and a transmission medium such as the Internet.

**[0200]** In other words, in the embodiment, each of the constituent elements may be formed of dedicated hardware and implemented by executing software which is suitable to each constituent element. For example, each of the constituent elements may be implemented by a program executing unit, such as a CPU or a processor, reading and executing a software program stored in a recording medium such as a hard disc or a semiconductor memory.

**[0201]** In other words, each of the constituent elements in the unauthorized connection detecting device shown in FIG. 2 or FIG. 14 may be implemented in the form of software. Then, the software to implement an unauthorized connection detecting device in the embodiment is a program to cause a computer to execute the steps included in the unauthorized connection detecting method below. In other words, the unauthorized connection detecting method is employed by an unauthorized connection detecting device for detecting whether or not a power storage device that is connectable to a charge/discharge device for charging or discharging with power is an unauthorized power storage device. The unauthorized connection detecting method includes: receiving by the unauthorized connection detecting device first charge/discharge information in which first identification information and first connection information are associated each other, the first identification information being information for identifying an encryption key of the power storage device used for mutual authentication between the charge/discharge device and the power storage device connectable to the charge/discharge device, and the first connection information being information on the power storage device and obtained when the power storage

device is connected to the charge/discharge device; and detecting by the unauthorized connection detecting device whether or not the power storage device connected to the charge/discharge device is the unauthorized power storage device, by determining, using the first identification information and the first connection information included in the received first charge/discharge information, whether or not two or more power storage devices associated with a single first identification information item are present.

**[0202]** Moreover, the unauthorized connection detecting method is employed by an unauthorized connection detecting device for detecting whether or not a charge/discharge device that is connectable with a power storage device and charges or discharges the power storage device is an unauthorized charge/discharge device. The unauthorized connection detecting method includes: receiving by the unauthorized connection detecting device second charge/discharge information in which second identification information and second connection information are associated each other, the second identification information being information for identifying an encryption key of the charge/discharge device used for mutual authentication between the power storage device and the charge/discharge device connectable with the power storage device, and the second connection information being information on the charge/discharge device and obtained when the charge/discharge device is connected with the power storage device; and detecting by the unauthorized connection detecting device whether or not the charge/discharge device connected with the power storage device is the unauthorized charge/discharge device, by determining, using the second identification information and the second connection information included in the received second charge/discharge information, whether or not two or more charge/discharge devices associated with a single second identification information item are present.

**[0203]** In addition, each of the processing units included in an unauthorized connection detecting device according to an implementation of the present invention may be implemented in the form of an integrated circuit; namely, the large scale integration (LSI). In other words, each of the processing units included in FIG. 2 or FIG. 14 may made as separate individual chips, or as a single chip to include a part or all of the processing units.

**[0204]** Furthermore, here, LSI is mentioned but there are instances where, due to a difference in the degree of integration, the designations IC, LSI, super LSI, and ultra LSI are used.

**[0205]** Furthermore, the means for circuit integration is not limited to the LSI, and implementation in the form of a dedicated circuit or a general-purpose processor is also available. In addition, it is also acceptable to use a Field Programmable Gate Array (FPGA) that is programmable after the LSI has been manufactured, and a reconfigurable processor in which connections and settings of circuit cells within the LSI are reconfigurable.

**[0206]** Furthermore, if an integrated circuit technology that replaces the LSI appears thorough the progress in the semiconductor technology or an other derived technology, that technology can naturally be used to carry out integration of the constituent elements. Biotechnology can be applied to the integrated circuit technology.

[Industrial Applicability]

**[0207]** The present invention is applicable to an unauthorized connection detecting device which is capable of detecting an unauthorized power storage device or an unauthorized charge/discharge device that have a cryptographic module of an authentic product introduced thereinto in an unauthorized manner.

[Reference Signs List]

**[0208]**

| | |
|---|---|
| 10 | Unauthorized connection detecting system |
| 100, 101 | Unauthorized connection detecting device |
| 110 | Communications unit |
| 120 | Unauthorization detecting unit |
| 130 | Control unit |
| 140 | Storage unit |
| 141 | Secret key data |
| 142 | Public key certificate |
| 143 | First charge/discharge information |
| 144 | Second charge/discharge information |
| 200 | Charge/discharge device |
| 210 | Communications unit |
| 220 | Certificate information obtaining unit |
| 230 | Certificate verification unit |
| 240 | Time information detecting unit |
| 250 | Position information detecting unit |
| 260 | Control unit |
| 270 | Storage unit |
| 271 | Secret key data |
| 272 | Public key certificate |
| 273 | First charge/discharge information |
| 300 | Power storage device |
| 310 | Communications unit |
| 320 | Certificate information obtaining unit |
| 330 | Certificate verification unit |
| 340 | Charge/discharge device identification information obtaining unit |
| 350 | Power storage device identification information obtaining unit |
| 360 | Control unit |
| 370 | Storage unit |
| 371 | Secret key data |
| 372 | Public key certificate |
| 373 | Second charge/discharge information |
| 400 | House |
| 500 | Charging station |
| 600 | Communications network |

## Claims

1. An unauthorized connection detecting device which detects whether or not a power storage device that is connectable to a charge/discharge device for charging or discharging with power is an unauthorized power storage device, the unauthorized connection detecting device comprising:

   a communications unit configured to receive first charge/discharge information in which first identification information and first connection information are associated each other, the first identification information being information for identifying an encryption key of the power storage device used for mutual authentication between the charge/discharge device and the power storage device connectable to the charge/discharge device, and the first connection information being information on the power storage device and obtained when the power storage device is connected to the charge/discharge device; and
   an unauthorization detecting unit configured to detect whether or not the power storage device connected to the charge/discharge device is the unauthorized power storage device, by determining, using the first identification information and the first connection information included in the received first charge/discharge information, whether or not two or more power storage devices associated with a single first identification information item are present.

2. The unauthorized connection detecting device according to Claim 1,
   wherein the communications unit is configured to receive the first charge/discharge information in which the first identification information and the first connection information are associated each other, the first connection information including information indicating a time and a position when and where the power storage device was charged or discharged, and
   the unauthorization detecting unit is configured to detect whether or not the power storage device connected to the charge/discharge device is the unauthorized power storage device, by determining, based on a relationship between times and positions included in a first connection information item associated with a single first identification information item, whether or not two or more power storage devices associated with the single first identification information item are present, the first connection information item being included in the first connection information, and the first connection information item and the single first identification information item being included in the received first charge/discharge information.

3. The unauthorized connection detecting device according to Claim 2,
   wherein the communications unit is configured to receive the first charge/discharge information in which the first identification information, time information, and position information are associated one another, the time information indicating a time when the charge/discharge device charged or discharged the power storage device, and the position information indicating a position where the charge/discharge device was.

4. An unauthorized connection detecting device which detects whether or not a charge/discharge device that is connectable with a power storage device and charges or discharges the power storage device is an unauthorized charge/discharge device, the unauthorized connection detecting device comprising:

   a communications unit configured to receive second charge/discharge information in which second identification information and second connection information are associated each other, the second identification information being information for identifying an encryption key of the charge/discharge device used for mutual authentication between the power storage device and the charge/discharge device connectable with the power storage device, and the second connection information being information on the charge/discharge device and obtained when the charge/discharge device is connected with the power storage device; and
   an unauthorization detecting unit configured to detect whether or not the charge/discharge device connected with the power storage device is the unauthorized charge/discharge device, by determining, using the second identification information and the second connection information included in the received second charge/discharge information, whether or not two or more charge/discharge devices associated with a single second identification information item are present.

5. The unauthorized connection detecting device according to Claim 4,
   wherein the communications unit is configured to receive the second charge/discharge information in which the second identification information and the second connection information are associated each other, the second connection information including charge/discharge device identification information identifying the charge/discharge device, and
   the unauthorization detecting unit is configured to detect whether or not the charge/discharge device connected with the power storage device is the unauthorized charge/discharge device, by determining

whether or not two or more charge/discharge device identification information items, included in a second connection information item associated with a single second identification information item, indicate mutually different charge/discharge devices, thereby determining whether or not two or more charge/discharge devices associated with the single second identification information item are present, the two or more charge/discharge device identification information items being included in the charge/discharge device identification information, the second connection information item being included in the second connection information, and the second connection information item and the single second identification item being included in the received second charge/discharge information.

**6.** The unauthorized connection detecting device according to Claim 5,
wherein the communications unit is configured to receive the second charge/discharge information in which the second identification information and the second connection information are associated each other, the second connection information including, as the charge/discharge device identification information, position information indicating a position of the charge/discharge device, and
the unauthorization detecting unit is configured to detect whether or not the charge/discharge device connected with the power storage device is the unauthorized charge/discharge device, by determining whether or not two or more position information items, included in a second connection information item associated with a single second identification information item, indicate mutually different positions, thereby determining whether or not two or more charge/discharge devices associated with the single second identification information item are present, the two or more position information items being included in the position information, the second connection-information item being included in the second connection information, and the second connection information item and the single second identification information item being included in the received second charge/discharge information.

**7.** The unauthorized connection detecting device according to Claim 5,
wherein the communications unit is configured to receive the second charge/discharge information in which the second identification information and the second connection information are associated each other, the second connection information including direct current information indicating, as the charge/discharge device identification information, a fluctuation of a direct current provided from the charge/discharge device, and
the unauthorization detecting unit is configured to detect whether or not the charge/discharge device connected with the power storage device is the unauthorized charge/discharge device, by determining whether or not two or more direct current information items, included in a second connection information item associated with a single second identification information item, indicate mutually different fluctuations, thereby determining whether or not two or more charge/discharge devices associated with the single second identification information item, the two or more direct current information items being included in the direct current information, the second connection information item being included in the second connection information, and the second connection information item and the single second identification information item being included in the received second charge/discharge information.

**8.** The unauthorized connection detecting device according to any one of Claims 4 to 7,
wherein the communications unit is configured to receive the second charge/discharge information in which the second identification information and the second connection information are associated each other, the second connection information including the power storage device identification information identifying the power storage device connected to the charge/discharge device, and
the unauthorization detecting unit is configured to detect whether or not the charge/discharge device connected with the power storage device is the unauthorized charge/discharge device, by determining whether or not the number of power storage devices, identified by two or more power storage device identification information items included in a second connection information item associated with a single second identification information item, is larger than or equal to a predetermined threshold, thereby determining whether or not two or more charge/discharge devices associated with the single second identification information item are present, the two or more power storage device identification information items being included in the power storage device identification information, the second connection information item being included in the second connection information, and the second connection information item and the single second identification information item being included in the received second charge/discharge information.

**9.** The unauthorized connection detecting device according to any one of Claims 1 to 8,
wherein the communications unit is configured to receive information via one of a communications network connected with a charge station for charging the power storage device when the power storage device is connected and a communications network connected to the charge/discharge device.

**10.** An unauthorized connection detecting system which detects whether or not a power storage device is an unauthorized power storage device, the unauthorized connection detecting system comprising:

a charge/discharge device which charges or discharges with power; and
the unauthorized connection detecting device according to any one of Claims 1 to 3 and 9 which detects whether or not a power storage device that is connectable to the charge/discharge device is an unauthorized power storage device.

**11.** An unauthorized connection detecting system which detects whether or not a charge/discharge device for charging or discharging with power is an unauthorized charge/discharge device, the unauthorized connection detecting system comprising:

a power storage device; and
an unauthorized connection detecting device according to any one of Claims 4 to 9 which detects whether or not a charge/discharge device that is connectable with the power storage device and charges or discharges the power storage device is an unauthorized charge/discharge device.

**12.** An unauthorized connection detecting method employed by an unauthorized connection detecting device for detecting whether or not a power storage device that is connectable to a charge/discharge device for charging or discharging with power is an unauthorized power storage device, the unauthorized connection detecting method comprising:

receiving by the unauthorized connection detecting device first charge/discharge information in which first identification information and first connection information are associated each other, the first identification information being information for identifying an encryption key of the power storage device used for mutual authentication between the charge/discharge device and the power storage device connectable to the charge/discharge device, and the first connection information being information on the power storage device and obtained when the power storage device is connected to the charge/discharge device; and
detecting by the unauthorized connection detecting device whether or not the power storage device connected to the charge/discharge device is the unauthorized power storage device, by determining, using the first identification information and the first connection information included in the received first charge/discharge information, whether or not two or more power storage devices associated with a single first identification information item are present.

**13.** An unauthorized connection detecting method employed by an unauthorized connection detecting device for detecting whether or not a charge/discharge device that is connectable with a power storage device and charges or discharges the power storage device is an unauthorized charge/discharge device, the unauthorized connection detecting device comprising:

receiving by the unauthorized connection detecting device second charge/discharge information in which second identification information and second connection information are associated each other, the second identification information being information for identifying an encryption key of the charge/discharge device used for mutual authentication between the power storage device and the charge/discharge device connectable with the power storage device, and the second connection information being information on the charge/discharge device and obtained when the charge/discharge device is connected with the power storage device; and
detecting by the unauthorized connection detecting device whether or not the charge/discharge device connected with the power storage device is the unauthorized charge/discharge device, by determining, using the second identification information and the second connection information included in the received second charge/discharge information, whether or not two or more charge/discharge devices associated with a single second identification information item are present.

**14.** A program which causes a computer to execute the steps included in the unauthorized connection detecting method according to one of Claims 12 and 13.

**15.** A computer-readable recording medium which records the program according to Claim 14.

**16.** An integrated circuit which detects whether or not a power storage device that is connectable to a charge/discharge device for charging or discharging with power is an unauthorized power storage device, the integrated circuit comprising:

a communications unit configured to receive first charge/discharge information in which first identification information and first connection information are associated each other, the first identification information being information for identifying an encryption key of the power storage

device used for mutual authentication between the charge/discharge device and the power storage device connectable to the charge/discharge device, and the first connection information being information on the power storage device and obtained when the power storage device is connected to the charge/discharge device; and
an unauthorization detecting unit configured to detect whether or not the power storage device connected to the charge/discharge device is the unauthorized power storage device, by determining, using the first identification information and the first connection information included in the received first charge/discharge information, whether or not two or more power storage devices associated with a single first identification information item are present.

**17.** An integrated circuit which detects whether or not a charge/discharge device that is connectable with a power storage device and charges or discharges the power storage device is an unauthorized charge/discharge device, the integrated circuit comprising:

a communications unit configured to receive second charge/discharge information in which second identification information and second connection information are associated each other, the second identification information being information for identifying an encryption key of the charge/discharge device used for mutual authentication between the power storage device and the charge/discharge device connectable with the power storage device, and the second connection information being information on the charge/discharge device and obtained when the charge/discharge device is connected with the power storage device; and
an unauthorization detecting unit configured to detect whether or not the charge/discharge device connected with the power storage device is the unauthorized charge/discharge device, by determining, using the second identification information and the second connection information included in the received second charge/discharge information, whether or not two or more charge/discharge devices associated with a single second identification information item are present.

FIG. 1

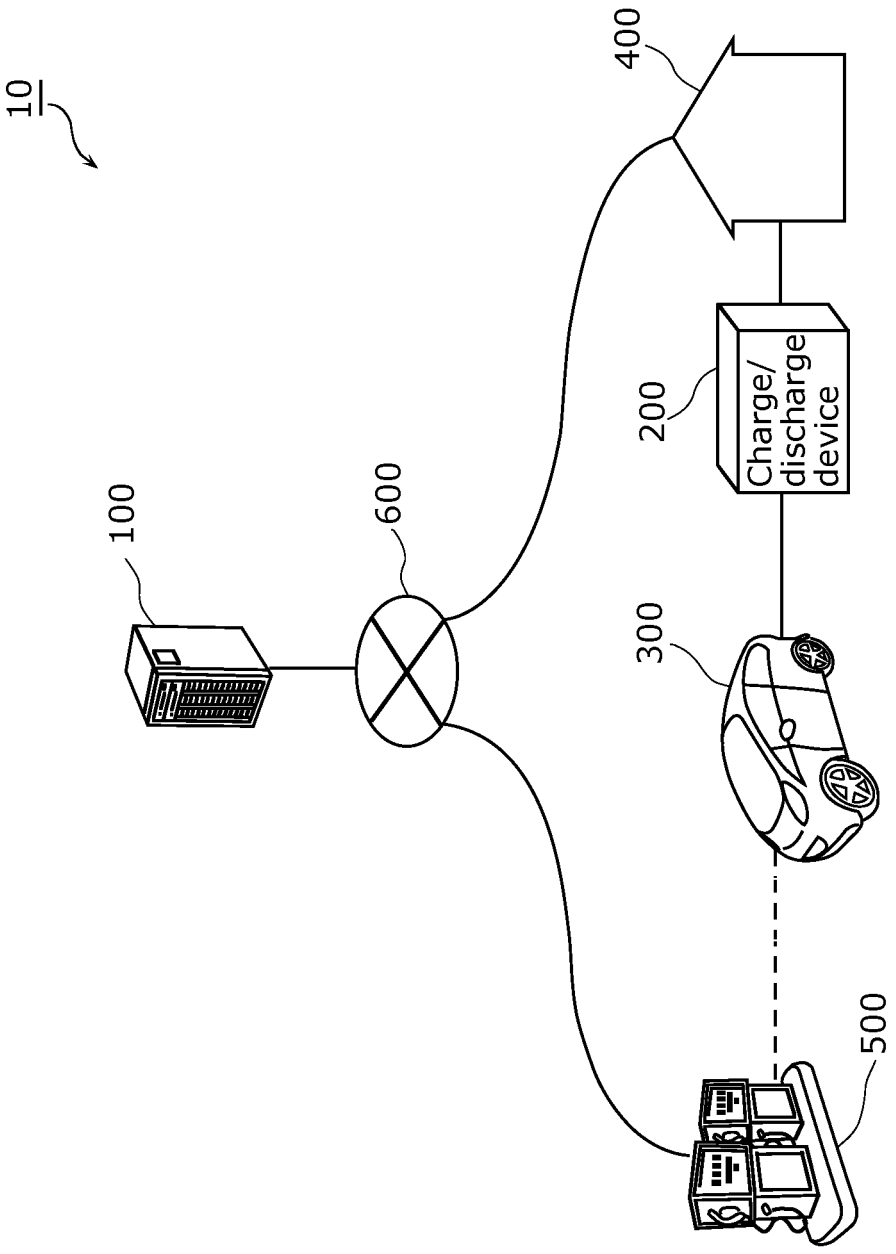


FIG. 2

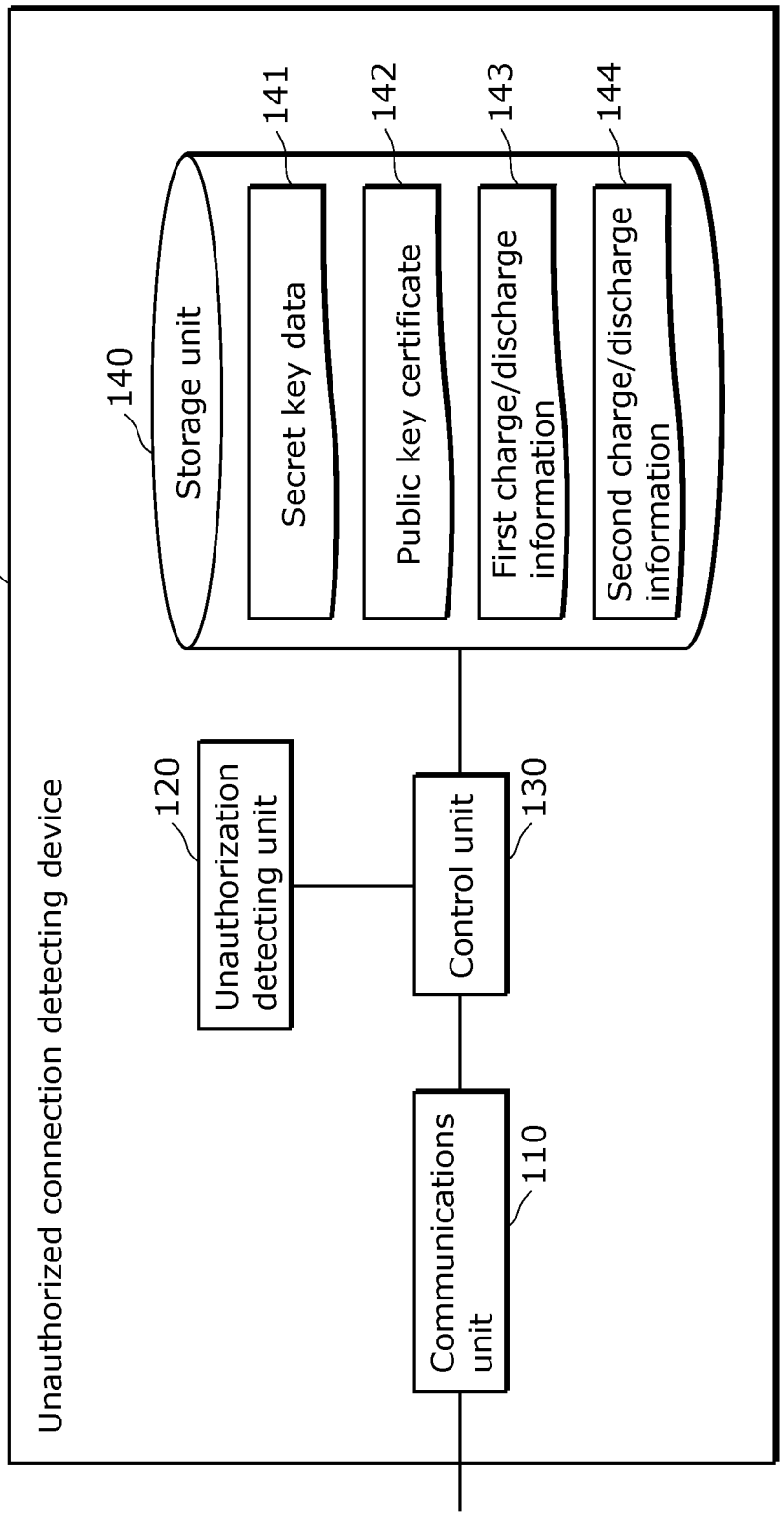

100
Unauthorized connection detecting device
140
Storage unit
141
Secret key data
142
Public key certificate
143
First charge/discharge information
144
Second charge/discharge information
120
Unauthorization detecting unit
130
Control unit
110
Communications unit

FIG. 3

143

| First identification information | First connection information | |
|---|---|---|
| | Time information | Position information |
| ID11 | T11 | P11 |
| | T12 | P12 |
| | T13 | P13 |
| | ⋮ | ⋮ |
| ID12 | T21 | P21 |
| | T22 | P22 |
| | T23 | P23 |
| | ⋮ | ⋮ |
| ⋮ | ⋮ | ⋮ |

FIG. 4

144

| Second identification information | Second connection information | |
|---|---|---|
| | Charge/discharge device identification information | Power storage device identification information |
| ID21 | A11 | B11 |
| | A12 | B12 |
| | A13 | B13 |
| | ⋮ | ⋮ |
| ID22 | A21 | B21 |
| | A22 | B22 |
| | A23 | B23 |
| | ⋮ | ⋮ |
| ⋮ | ⋮ | ⋮ |

FIG. 5

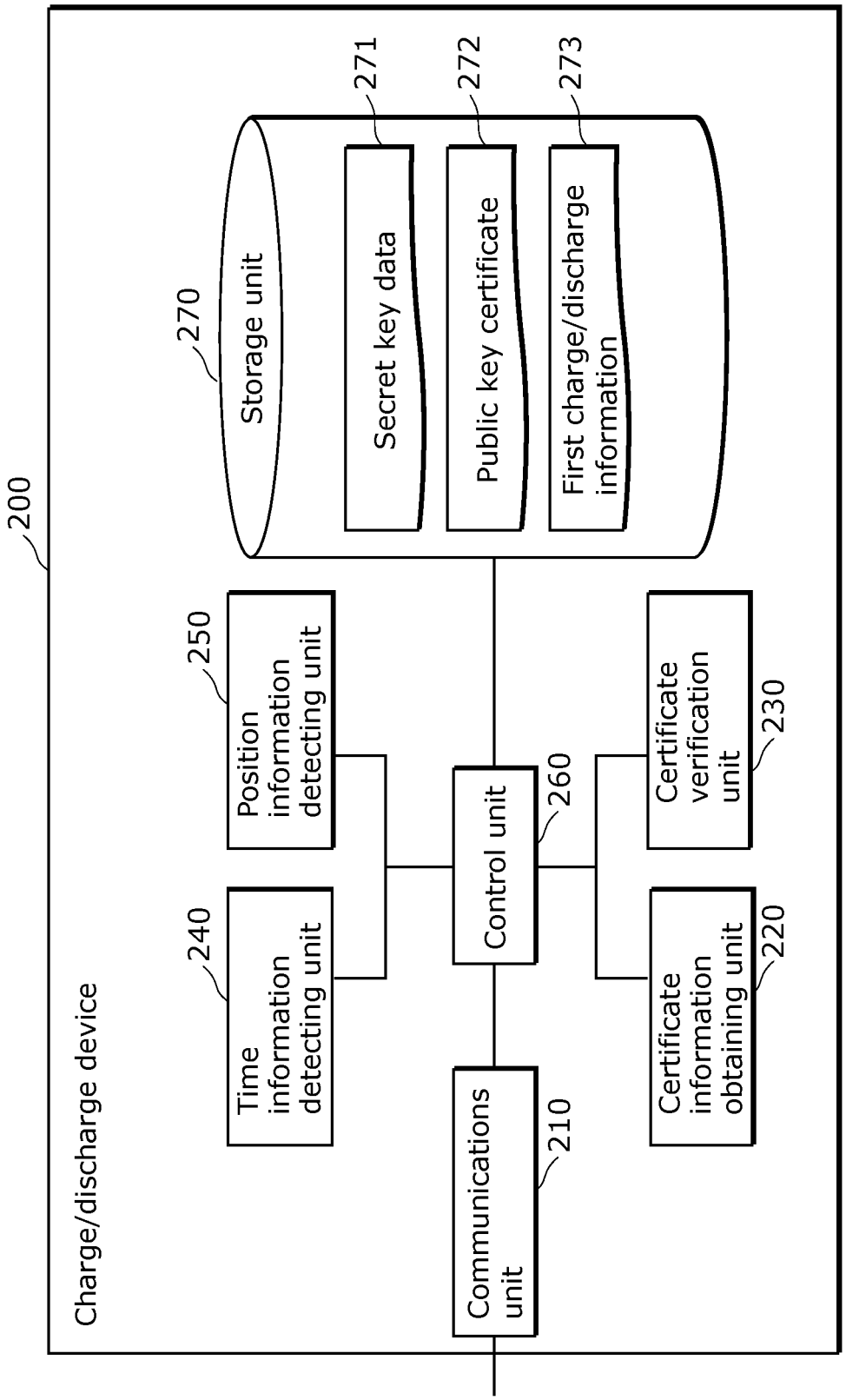

200
Charge/discharge device
270
Storage unit
271
Secret key data
272
Public key certificate
273
First charge/discharge information
250
Position information detecting unit
240
Time information detecting unit
260
Control unit
230
Certificate verification unit
220
Certificate information obtaining unit
210
Communications unit

FIG. 6

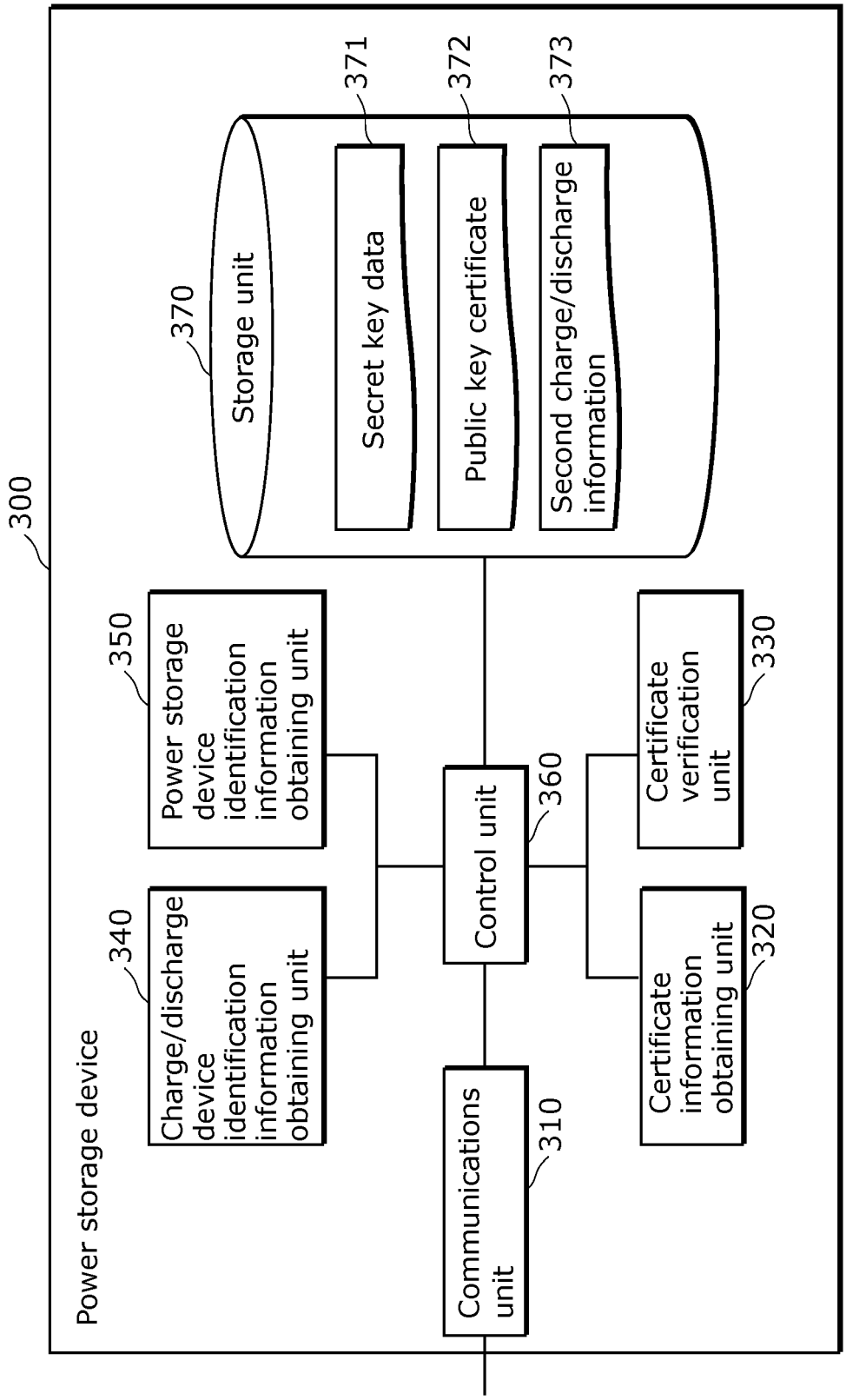

Power storage device
300
Storage unit
370
Secret key data
371
Public key certificate
372
Second charge/discharge information
373
Power storage device identification information obtaining unit
350
Charge/discharge device identification information obtaining unit
340
Control unit
360
Certificate verification unit
330
Certificate information obtaining unit
320
Communications unit
310

FIG. 7

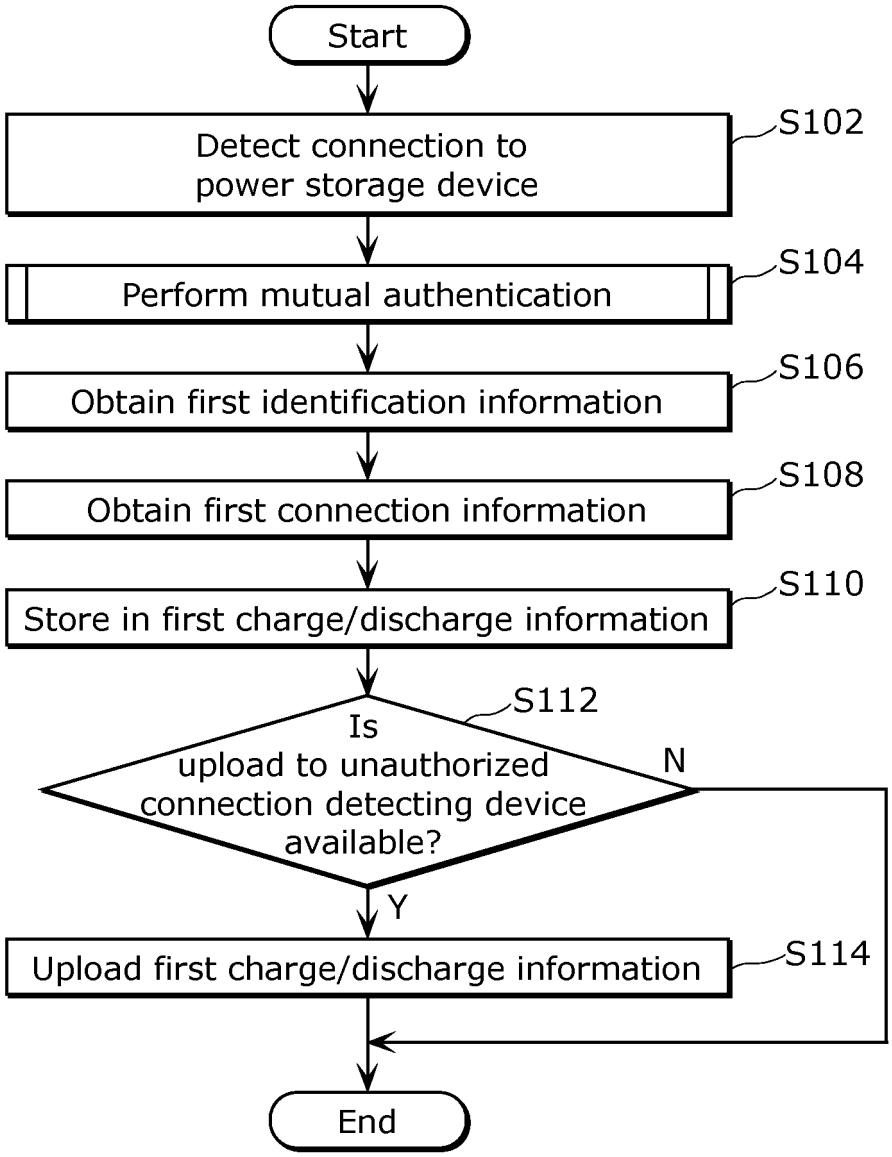

Start
Detect connection to power storage device
S102
Perform mutual authentication
S104
Obtain first identification information
S106
Obtain first connection information
S108
Store in first charge/discharge information
S110
Is upload to unauthorized connection detecting device available?
S112
N
Y
Upload first charge/discharge information
S114
End

FIG. 8

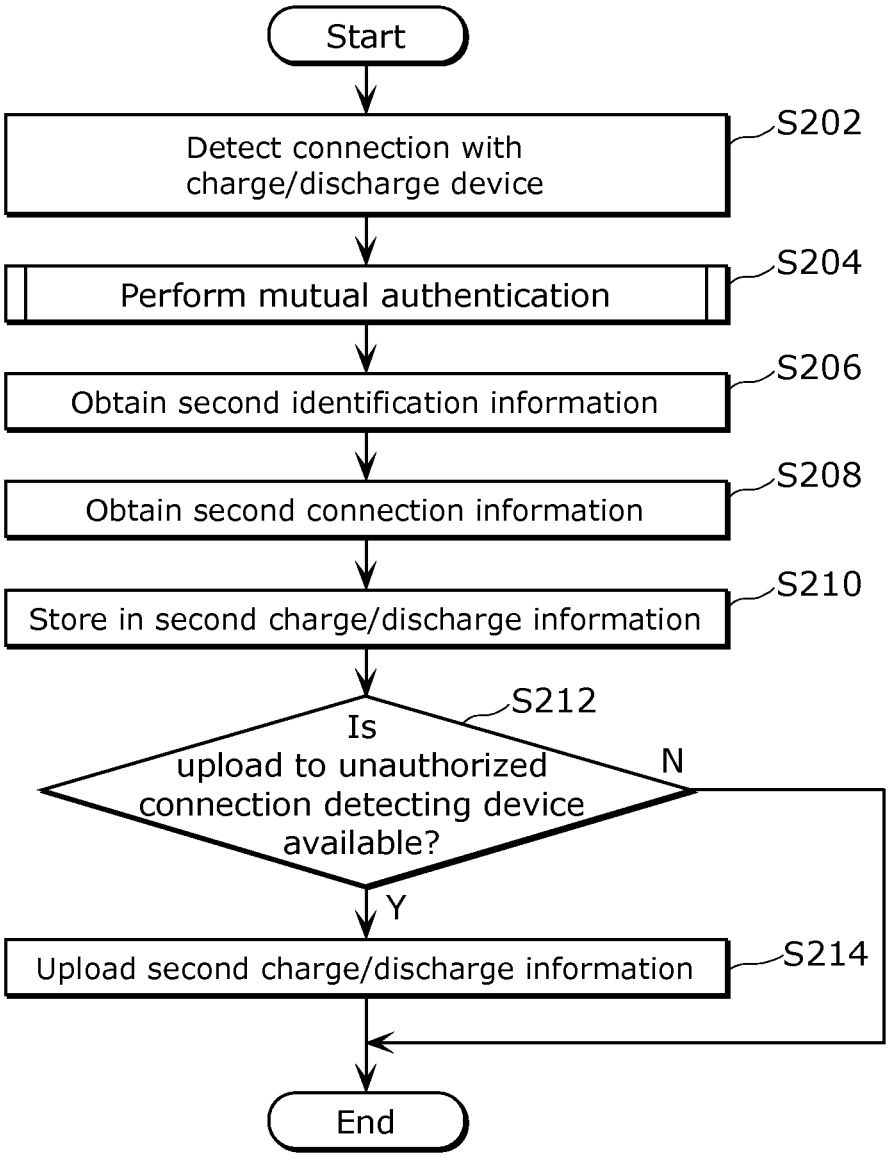

Start
Detect connection with charge/discharge device
S202
Perform mutual authentication
S204
Obtain second identification information
S206
Obtain second connection information
S208
Store in second charge/discharge information
S210
Is upload to unauthorized connection detecting device available?
S212
N
Y
Upload second charge/discharge information
S214
End

FIG. 9

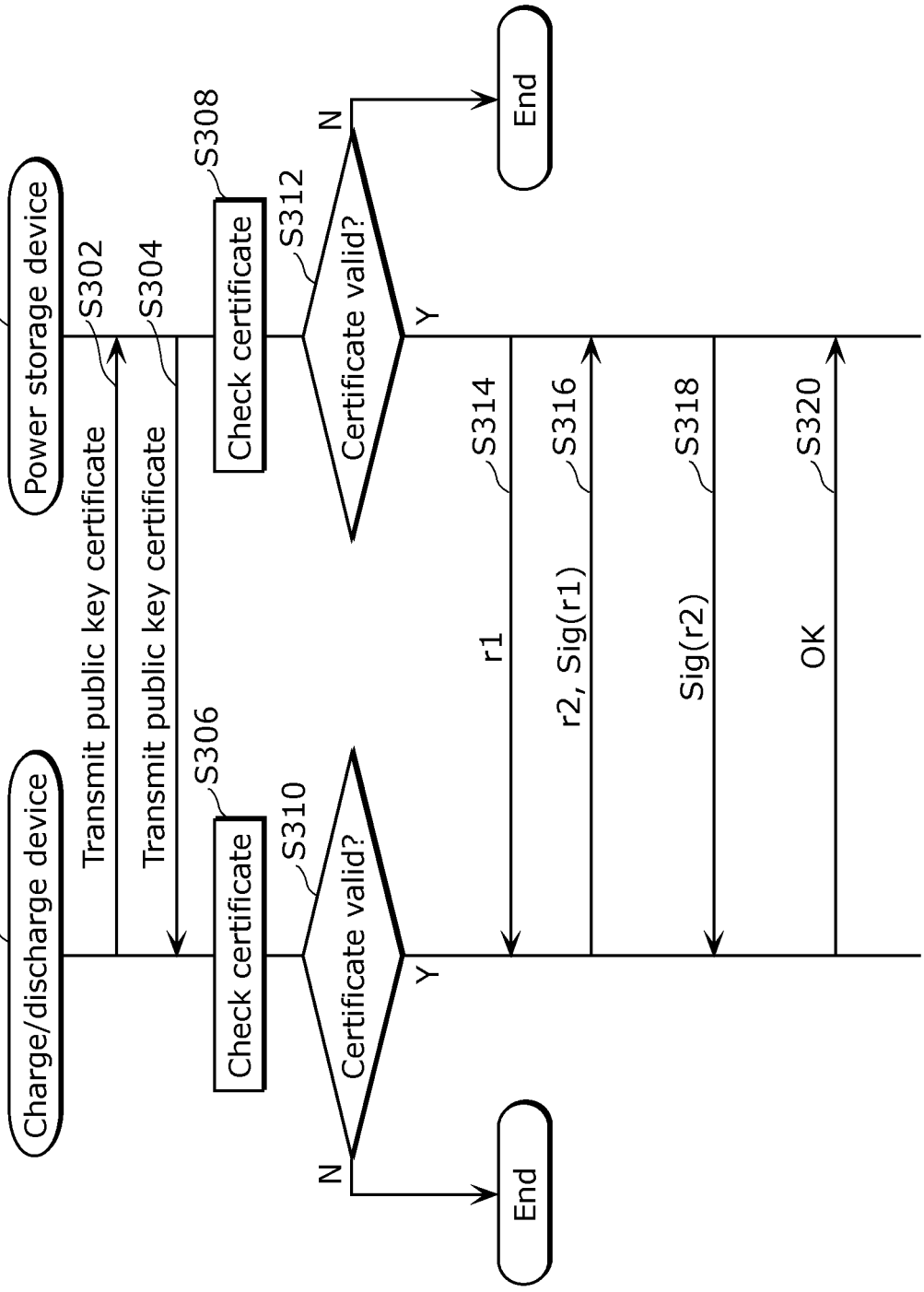

Charge/discharge device
200
Power storage device
300
Transmit public key certificate
S302
Transmit public key certificate
S304
Check certificate
S306
Check certificate
S308
Certificate valid?
S310
Certificate valid?
S312
N
Y
N
Y
End
End
r1
S314
r2, Sig(r1)
S316
Sig(r2)
S318
OK
S320

FIG. 10

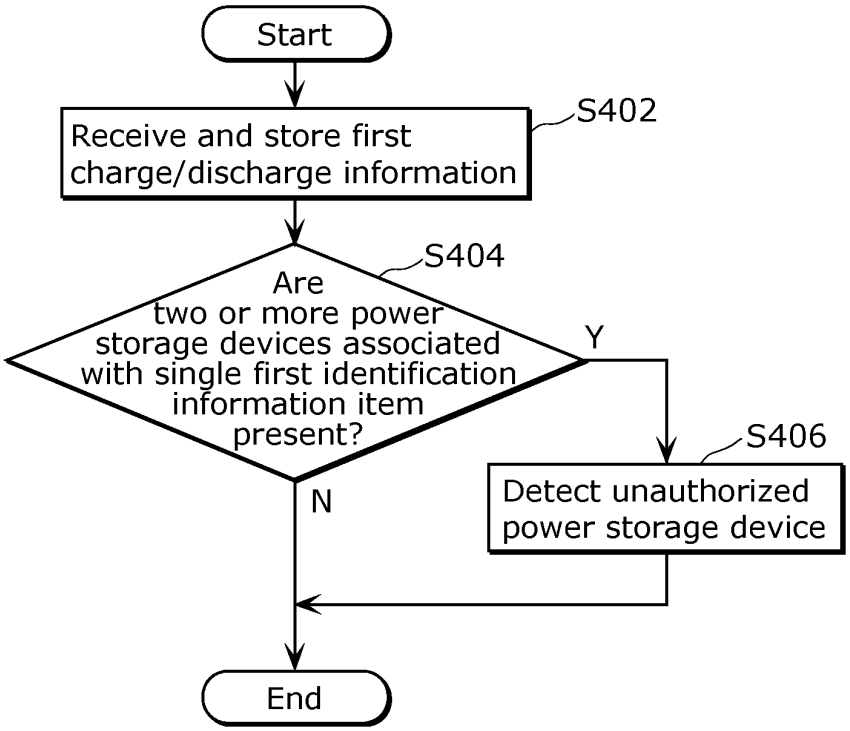

Start
Receive and store first charge/discharge information
S402
Are two or more power storage devices associated with single first identification information item present?
S404
Y
N
Detect unauthorized power storage device
S406
End

FIG. 11

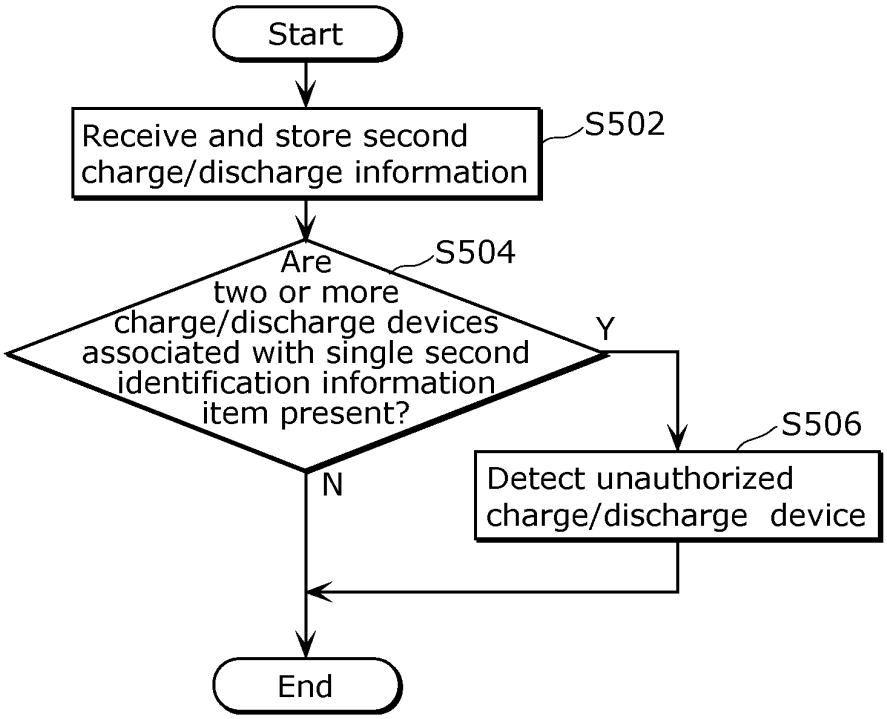

Start
Receive and store second charge/discharge information
S502
Are two or more charge/discharge devices associated with single second identification information item present?
S504
Y
N
Detect unauthorized charge/discharge device
S506
End

FIG. 12

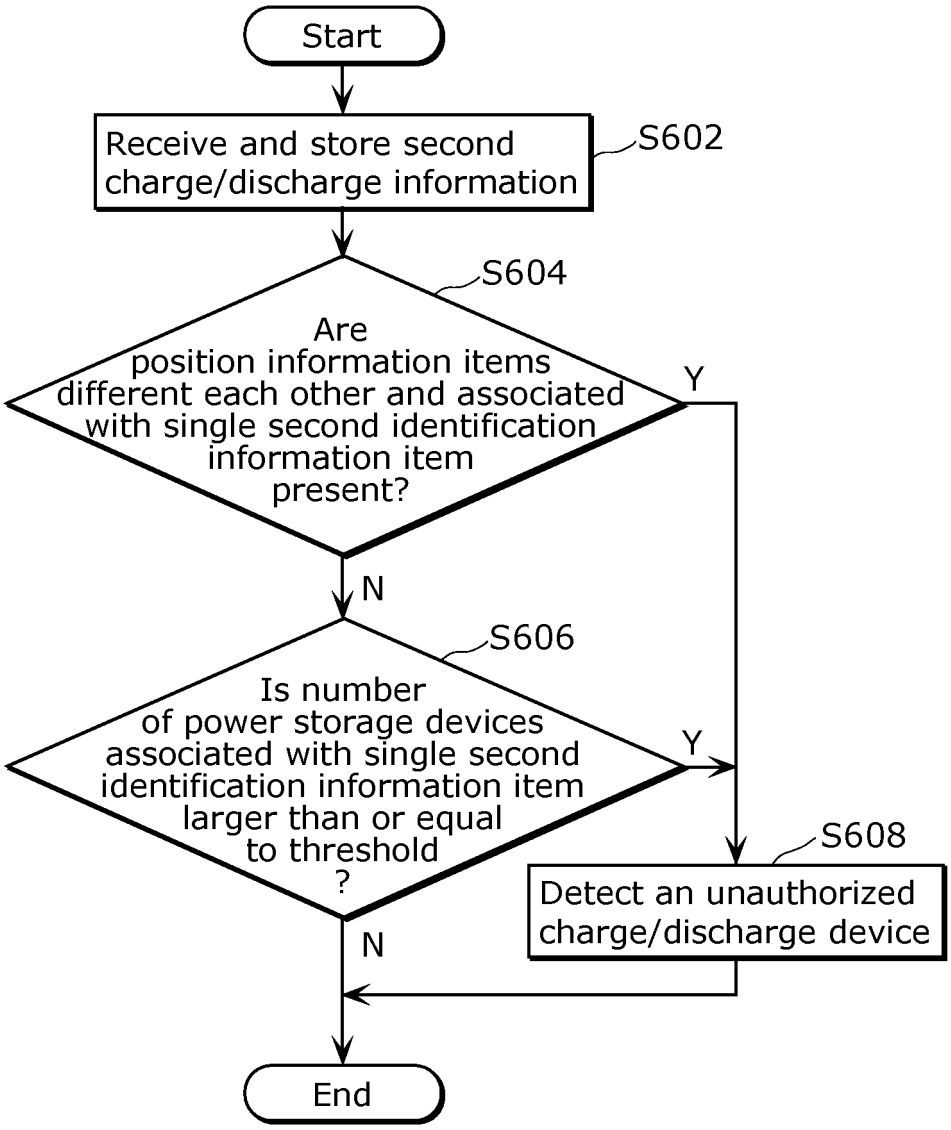

Start
Receive and store second charge/discharge information
S602
S604
Are position information items different each other and associated with single second identification information item present?
Y
N
S606
Is number of power storage devices associated with single second identification information item larger than or equal to threshold ?
Y
N
S608
Detect an unauthorized charge/discharge device
End

FIG. 13

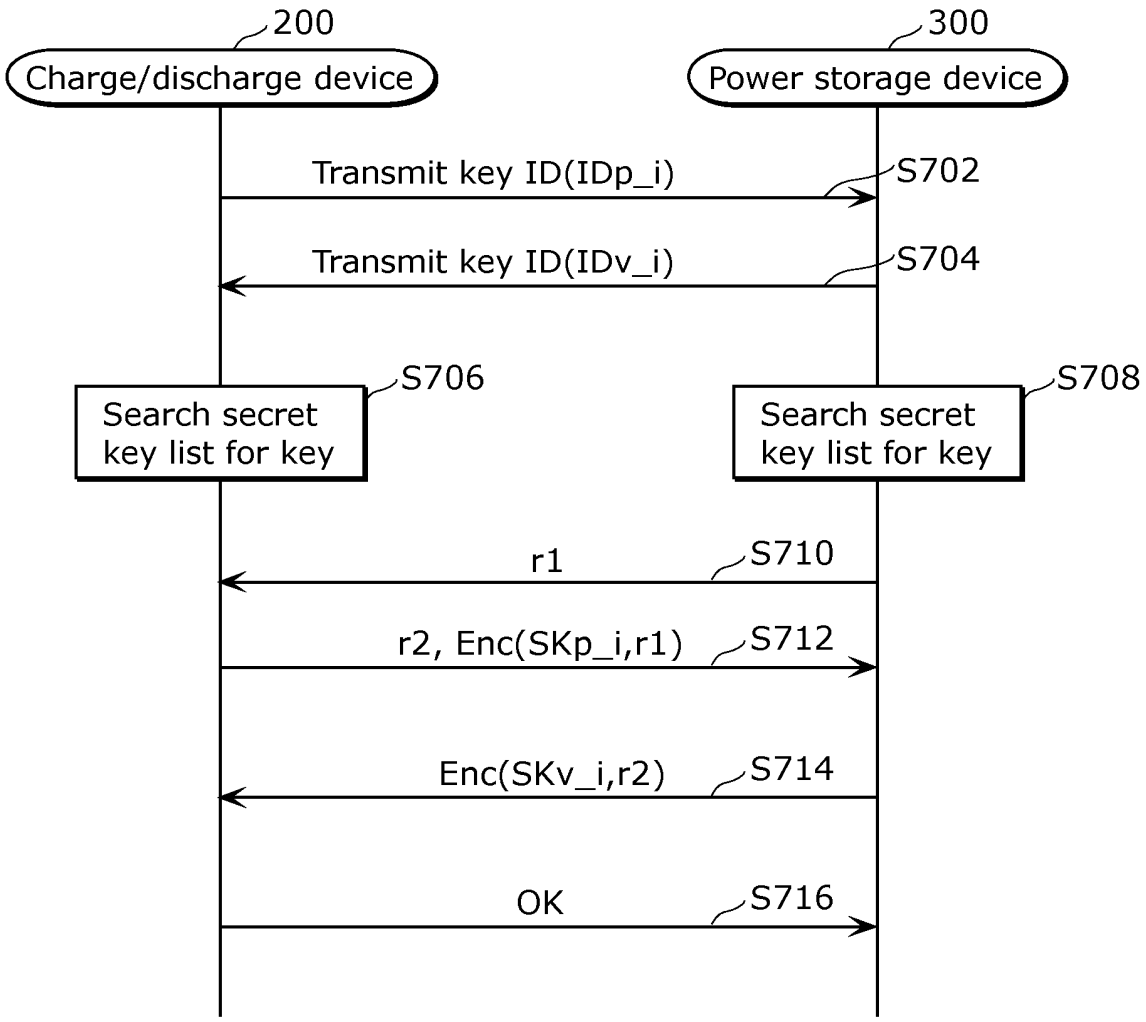
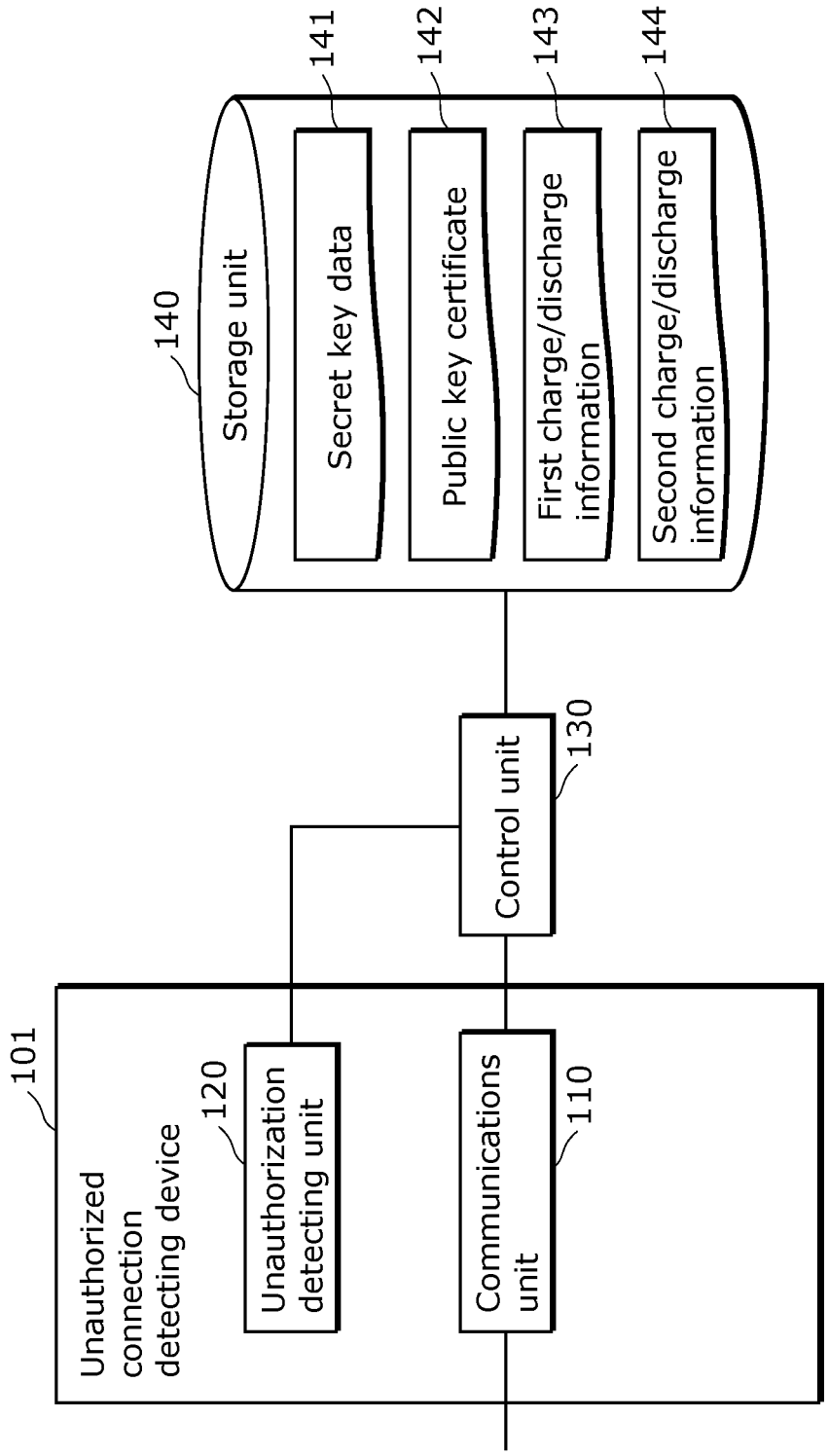

200
Charge/discharge device
300
Power storage device
Transmit key ID(IDp_i)
S702
Transmit key ID(IDv_i)
S704
S706
Search secret key list for key
S708
Search secret key list for key
r1
S710
r2, Enc(SKp_i,r1)
S712
Enc(SKv_i,r2)
S714
OK
S716

FIG. 14


101
Unauthorized connection detecting device
120
Unauthorization detecting unit
110
Communications unit
130
Control unit
140
Storage unit
141
Secret key data
142
Public key certificate
143
First charge/discharge information
144
Second charge/discharge information

## INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2012/007076

A. CLASSIFICATION OF SUBJECT MATTER
*H02J7/02*(2006.01)i, *B60L11/18*(2006.01)i, *H01M10/48*(2006.01)i, *H02J7/00*(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H02J7/02, B60L11/18, H01M10/48, H02J7/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2012
Kokai Jitsuyo Shinan Koho 1971-2012 Toroku Jitsuyo Shinan Koho 1994-2012

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | JP 2006-331815 A (NEC Corp.), 07 December 2006 (07.12.2006), paragraphs [0014], [0027] to [0032]; fig. 1 to 2 (Family: none) | 1-17 |
| A | JP 2007-305074 A (Sony Corp.), 22 November 2007 (22.11.2007), paragraph [0005] & US 2009/0125979 A1 & EP 2023261 A1 & WO 2007/132908 A1 & KR 10-2009-0010202 A & CN 101443778 A & TW 200813699 A | 1-17 |

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 13 December, 2012 (13.12.12) | 25 December, 2012 (25.12.12) |
| Name and mailing address of the ISA/ Japanese Patent Office<br>Facsimile No. | Authorized officer<br>Telephone No. |

Form PCT/ISA/210 (second sheet) (July 2009)

## REFERENCES CITED IN THE DESCRIPTION

*This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.*

### Patent documents cited in the description


- JP 4407753 B **[0003]**
- JP 2010200528 A **[0003]**